

NOTICE: You and your company have obtained access to this report on the description of the system of Microsoft Corporation (the “Service Organization” or “Microsoft”) relating to in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters (“Azure”) for the Azure and Azure Government cloud environments, on controls for the period July 1, 2022, through June 30, 2023 (“this SOC 1 Report”) by accepting the terms of the Access Agreement that was attached to this SOC 1 Report and acknowledging that your company is a prospective customer of Microsoft or a prospective customer of a service where Azure is a component of the service. The terms of the Access Agreement include, among other things, an agreement by you and your company not to further disclose, distribute, quote, or reference this SOC 1 Report and an agreement to release and indemnify Deloitte & Touche LLP (“Deloitte & Touche”), its subsidiaries and its subcontractors, and their respective personnel. By reading this SOC 1 Report, you reconfirm your agreement to the terms of such Access Agreement. If you are not a prospective customer of Microsoft or a prospective customer of a service where Azure is a component of the service, then you are not authorized to possess, read, or have access to this SOC 1 Report and should immediately return this SOC 1 Report to Microsoft.

This SOC 1 Report is intended only to be used by Microsoft’s existing clients during the period July 1, 2022, through June 30, 2023, and their external auditors (i.e., “user entities” during the period July 1, 2022, through June 30, 2023, and the “user auditors”, respectively, as stated in the independent service auditor’s report contained in this SOC 1 Report and defined in the American Institute of Certified Public Accountants’ Attestation Standards, International Auditing and Assurance Standards Board’s International Standard on Assurance Engagements (ISAE) 3402 (ISAE 3402), and standard 951 established by the Institut der Wirtschaftsprüfer) (“Permitted Users”). Deloitte & Touche, the entity that issued the independent service auditor’s report contained in this SOC 1 Report, its subsidiaries and subcontractors, and their respective personnel shall have no liability, duties, responsibilities or other obligations to any entity who may obtain this SOC 1 Report who is not a Permitted User, including, without limitation, any entity who obtains this SOC 1 Report in contemplation of contracting for services with Microsoft.

Deloitte & Touche, its subsidiaries and subcontractors, and their respective personnel have no responsibility for the description of the system of Microsoft, including the control objectives and the controls. Nor do Deloitte & Touche, its subsidiaries and subcontractors, and their respective personnel have any obligation to advise or consult with any entity regarding their access to this SOC 1 Report. Any use of this SOC 1 Report by a party other than a Permitted User (“Other Third Party”) is at the sole and exclusive risk of such Other Third Party and such Other Third Party cannot and shall not rely on this SOC 1 Report. This SOC 1 Report is not to be further disclosed, distributed, quoted, or referenced to any third party or included or incorporated by reference in any other document, including any securities filings.



NOTE: You may not distribute this SOC 1 report for Microsoft Azure to other parties, except where Microsoft Azure is a component of the services you deliver to your customers. In this circumstance, you may distribute this SOC 1 report to users / customers of your own services. You must provide recipients of this SOC 1 report written documentation of the function that Microsoft provides as it relates to your services. You must keep a complete and accurate record of entities and the personnel of such entities to whom this SOC 1 report is provided. You must promptly provide copies of such records to Microsoft or Deloitte & Touche LLP upon request. You must display or deliver the language in this paragraph or language that is substantially equivalent to this paragraph to recipients of this SOC 1 report for Microsoft Azure.



Microsoft Corporation - Azure Including Dynamics 365

(Azure & Azure Government)

System and Organization Controls Report

July 1, 2022 to June 30, 2023

This report, including the description of tests of controls and results thereof in Section IV is intended solely for the information and use of the Service Organization, user entities of the Service Organization's system related to in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters ("Azure") for the Azure and Azure Government cloud environments, during some or all of the period, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Table of Contents

Section I: Independent Service Auditor's Report	1
Section II: Management's Assertion	5
Section III: Description of Microsoft Azure System	8
Section IV: Information Provided by Independent Service Auditor Except for Control Objectives and Control Activities	78
Section V: Supplemental Information Provided by Microsoft	131

Section I: Independent Service Auditor's Report

Section I: Independent Service Auditor's Report

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Scope

We have examined the description of the system of Microsoft Corporation (the "Service Organization" or "Microsoft") related to in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters ("Azure") in Section III of the report for the Azure and Azure Government cloud environments¹, for processing user entities' transactions throughout the period July 1, 2022 to June 30, 2023 (the "Description"), and the suitability of the design and operating effectiveness of controls included in the Description to achieve the related control objectives also included in the Description, based on the criteria identified in Section II (the "Assertion"). The controls and control objectives included in the Description are those that management of Microsoft believes are likely to be relevant to user entities' internal control over financial reporting and the Description does not include those aspects of the system of Microsoft that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section V, "Supplemental Information Provided by Microsoft" that describes the Service Organization's Compliance, Infrastructure Redundancy and Data Durability, Data Backup and Recovery, E.U. Data Protection Directive, Additional Resources, Management's Response to Exceptions Noted, and User Entity Responsibilities, is presented by management of the Service Organization to provide additional information and is not a part of the Service Organization's description of its system made available to user entities during the period July 1, 2022 to June 30, 2023. The information included in Section V has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system and, accordingly, we express no opinion on it.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of the Service Organization's controls are suitably designed and operating effectively, along with related controls at the Service Organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section II of the report, the Service Organization has provided an assertion about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. The Service Organization is responsible for

¹ In-scope services and offerings and coverage periods are defined in the *Azure and Azure Government Report Scope and Boundary* and *Internal Supporting Services* subsections in Section III of this SOC 1 report. In-scope datacenters, edge sites, and coverage periods are defined in the *Regions Covered by this Report* subsection in Section III of this SOC 1 report.

preparing the Description and its assertion, including the completeness, accuracy, and method of presentation of the Description and the assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA") and International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board, and standard 951 established by the Institut der Wirtschaftsprüfer. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the Description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period July 1, 2022 to June 30, 2023. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on the criteria in management's assertion.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved.
- Evaluating the overall presentation of the Description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA. We applied the statements on quality control standards established by the AICPA and accordingly maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of

the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section IV of the report.

Opinion

In our opinion, in all material respects, based on the criteria described in the Service Organization's assertion in Section II of the report:

- a. The Description fairly presents the system related to Microsoft's in-scope services and offerings, for Azure and Azure Government cloud environments, that was designed and implemented throughout the period July 1, 2022 to June 30, 2023.
- b. The controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2022 to June 30, 2023, and user entities applied the complementary controls assumed in the design of the Service Organization's controls throughout the period July 1, 2022 to June 30, 2023.
- c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved, throughout the period July 1, 2022 to June 30, 2023, if complementary user entity controls assumed in the design of Service Organization's controls operated effectively throughout the period July 1, 2022 to June 30, 2023.

Restricted Use

This report, including the description of tests of controls and results in Section IV of the report, is intended solely for the information and use of management of the Service Organization, user entities of the Service Organization's system related to Microsoft's in-scope services and offerings, for Azure and Azure Government cloud environments during some or all of the period July 1, 2022 to June 30, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Deloitte & Touche LLP

August 17, 2023

Section II: Management's Assertion



Section II: Management's Assertion

We have prepared the description of the system of Microsoft Corporation (the "Service Organization" or "Microsoft") relating to in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters for Azure and Azure Government cloud environments (the "Description"), for user entities during some or all of the period July 1, 2022 to June 30, 2023², and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Microsoft's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of the user entities.

Description Criteria

We confirm, to the best of our knowledge and belief, that:

1. The Description fairly presents the Azure system made available to user entities of the system during some or all of the period July 1, 2022 to June 30, 2023, for processing their transactions. The criteria we used in making this assertion were that the Description:
 - a. Presents how the system made available to user entities was designed and implemented to process relevant transactions, including, if applicable:
 - i. The types of services provided including, as appropriate, the classes of transactions processed.
 - ii. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - iii. The information used in the performance of procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - iv. How the system captures and addresses significant events and conditions.
 - v. The process used to prepare reports or other information provided to user entities of the system.
 - vi. Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
 - vii. The specified control objectives and controls designed to achieve those objectives, including, as

²In-scope services and offerings and coverage periods are defined in the *Azure and Azure Government Report Scope and Boundary* and *Internal Supporting Services* subsections in Section III of this SOC 1 report. In-scope datacenters, edge sites, and coverage periods are defined in the *Regions Covered by this Report* subsection in Section III of this SOC 1 report.

applicable, complementary user entity controls assumed in the design of the Service Organization's controls.

viii. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

- b. The Description includes relevant details of changes to Microsoft's system during the period covered by the Description when the Description covers a period of time.
 - c. The Description does not omit or distort information relevant to the Service Organization's system, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.
2. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period July 1, 2022 to June 30, 2023, to achieve those control objectives provided that user entities applied the controls contemplated in the design of the Service Organization's controls. The criteria we used in making this assertion were that:
- a. The risks that threaten the achievement of the control objectives stated in the Description have been identified by Microsoft.
 - b. Controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved.
 - c. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section III:

Description of Microsoft Azure System

Section III: Description of Microsoft Azure System

Overview of Operations

Business Description

Azure

Microsoft Azure is a cloud computing platform for building, deploying and managing applications through a global network of Microsoft and third-party managed datacenters. It supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud service models, and enables hybrid solutions that integrate cloud services with customers' on-premises resources. Microsoft Azure supports many customers, partners, and government organizations that span across a broad range of products and services, geographies, and industries. Microsoft Azure is designed to meet their security, confidentiality, and compliance requirements.

Microsoft datacenters support Microsoft Azure, Microsoft Dynamics 365, and Microsoft Online Services ("Online Services"). Online Services such as Intune, Power BI, and others are Software as a Service (SaaS) services that leverage the underlying Microsoft Azure platform and datacenter infrastructure. See section titled 'Azure and Azure Government Report Scope and Boundary' for the Microsoft Azure services and offerings and Online Services that are in scope for this report.

Dynamics 365

[Dynamics 365](#) is an online business application suite that integrates the Customer Relationship Management (CRM) capabilities and its extensions with the Enterprise Resource Planning (ERP) capabilities. These end-to-end business applications help customers turn relationships into revenue, earn customers, and accelerate business growth.

"Azure", when referenced in this report, comprises of "Microsoft Azure", "Microsoft Dynamics 365", "Online Services", and the supporting datacenters listed in this report.

Applicability of Report

The detail herein is limited to operational controls supporting Azure and Online Services as defined in the Azure and Azure Government Report Scope and Boundary described below. Azure services and offerings and supported Online Services in scope for this report are defined separately for the following environments: Azure and Azure Government.

Azure and Azure Government Report Scope and Boundary

[Azure](#) is global multi-tenant cloud platform that provides a public cloud deployment model. [Azure Government](#) is a US Government Community Cloud that is physically separated from the Azure cloud. The following Azure and Azure Government services and offerings are in scope for this report, for the period July 1, 2022 through June 30, 2023, unless otherwise indicated explicitly:

Product Category Offering / Service		Cloud Environment Scope	
		Azure	Azure Government
Microsoft Datacenters			
Microsoft Datacenter and Operations Service		✓	✓
Azure			
Compute	App Service	✓	✓
	Azure Arc Enabled Servers	✓	✓
	Azure Cloud Services	✓	✓
	Azure Functions	✓	✓
	Azure Service Fabric	✓	✓
	Azure VM Image Builder	✓	-
	Azure VMware Solution	✓	-
	Batch	✓	✓
	Machine Configuration	✓	✓
	Planned Maintenance	✓	✓
	Virtual Machines	✓	✓
	Virtual Machine Scale Sets	✓	✓
	Azure Virtual Desktop	✓	✓
Containers	Azure Arc Enabled Kubernetes	✓	✓
	Azure Container Apps ³	✓	-
	Azure Kubernetes Configuration Management	✓	✓
	Azure Kubernetes Service (AKS)	✓	✓
	Azure Red Hat OpenShift	✓	-
	Container Instances	✓	✓
	Azure Container Registry	✓	✓

³ Examination period for this offering / service for Azure and Azure Government was from October 1, 2022 to June 30, 2023.

Product Category	Offering / Service	Cloud Environment Scope	
		Azure	Azure Government
Networking	Application Gateway	✓	✓
	Azure Bastion	✓	✓
	Azure DDoS Protection	✓	✓
	Azure DNS	✓	✓
	Azure ExpressRoute	✓	✓
	Azure Firewall	✓	✓
	Azure Firewall Manager	✓	-
	Azure Front Door	✓	✓
	Azure Internet Analyzer	✓	-
	Azure Private Link	✓	✓
	Azure Route Server	✓	✓
	Azure Web Application Firewall	✓	✓
	Azure Content Delivery Network	✓	✓
	IP Services	✓	✓
	Azure Load Balancer	✓	✓
	Microsoft Azure Peering Service	✓	✓
	Network Watcher	✓	✓
	Traffic Manager	✓	✓
	Virtual Network	✓	✓
	Virtual Network NAT	✓	✓
	VPN Gateway	✓	✓
	Virtual WAN	✓	✓
Storage	Azure Archive Storage	✓	✓
	Azure Backup	✓	✓
	Azure Data Box	✓	✓
	Azure Data Lake Storage Gen1	✓	-

Product Category	Offering / Service	Cloud Environment Scope	
		Azure	Azure Government
	Azure File Sync	✓	✓
	Azure HPC Cache	✓	✓
	Azure Import/Export ⁴	✓	✓
	Azure NetApp Files	✓	✓
	Azure Site Recovery	✓	✓
	Azure Storage (Blobs (including Azure Data Lake Storage Gen2), Disks, Files, Queues, Tables, Azure Disk Storage) including Cool and Premium	✓	✓
	StorSimple	✓	✓
Databases	Azure Arc-Enabled SQL Server ³	✓	-
	Azure Cache for Redis	✓	✓
	Azure Cosmos DB	✓	✓
	Azure Database for MariaDB	✓	✓
	Azure Database for MySQL	✓	✓
	Azure Database for PostgreSQL	✓	✓
	Azure Database Migration Service	✓	✓
	Azure Health Data Services	✓	✓
	Azure SQL	✓	✓
	Azure Synapse Analytics	✓	✓
	Microsoft Azure Managed Instance for Apache Cassandra	✓	-
	SQL Server Registry ⁵	✓	-
	SQL Server Stretch Database	✓	✓

⁴ Examination period for this offering / service for Azure and Azure Government was from July 1, 2022 to March 31, 2023.

⁵ Examination period for this offering / service for Azure and Azure Government was from July 1, 2022 to September 30, 2022.

Product Category Offering / Service		Cloud Environment Scope	
		Azure	Azure Government
Developer Tools	Azure App Configuration	✓	✓
	Azure DevTest Labs	✓	✓
	Azure for Education	✓	-
	Azure Lab Services	✓	-
	Azure Load Testing	✓	-
	GitHub AE	✓	✓
Analytics	Azure Analysis Services	✓	✓
	Azure Data Explorer	✓	✓
	Azure Data Share	✓	✓
	Azure Stream Analytics	✓	✓
	Data Catalog	✓	-
	Azure Data Factory	✓	✓
	Data Lake Analytics	✓	-
	Azure HDInsight	✓	✓
	Power BI Embedded	✓	✓
AI + Machine Learning	AI Builder	✓	✓
	Azure Applied AI Services	✓	-
	Azure Bot Service	✓	✓
	Azure Open Datasets	✓	-
	Azure OpenAI Service	✓	-
	Azure Machine Learning	✓	✓
	Azure AI Services	✓	✓
	Azure AI Services: AI Anomaly Detector	✓	-
	Azure AI Services: Azure AI Vision	✓	✓
	Azure AI Services: Azure AI Content Safety	✓	✓
	Azure AI Services: Azure AI Custom Vision	✓	✓

Product Category Offering / Service		Cloud Environment Scope	
		Azure	Azure Government
	Azure AI Services: Face API	✓	✓
	Azure AI Services: Azure AI Document Intelligence	✓	✓
	Azure AI Services: Azure AI Immersive Reader	✓	-
	Azure AI Services: Conversational Language Understanding ³	✓	✓
	Azure AI Services: Azure AI Metrics Advisor	✓	-
	Azure AI Services: Azure AI Personalizer	✓	✓
	Azure AI Services: Question Answering	✓	✓
	Azure AI Services: Azure AI Speech	✓	✓
	Azure AI Services: Text Analytics	✓	✓
	Azure AI Services: Translator	✓	✓
	Azure AI Services: Azure AI Video Indexer	✓	✓
	Machine Learning Studio (Classic)	✓	-
	Autonomous Systems	✓	-
	Microsoft Genomics	✓	-
	Azure Health Bot	✓	-
Internet of Things	Azure Defender for IoT	✓	✓
	Azure Digital Twins	✓	-
	Azure IoT Central	✓	-
	Azure IoT Hub	✓	✓
	Azure Sphere	✓	-
	Azure Time Series Insights	✓	-
	Event Grid	✓	✓
	Event Hubs	✓	✓

Product Category Offering / Service		Cloud Environment Scope	
		Azure	Azure Government
	Microsoft Cloud for Sustainability	✓	-
	Notification Hubs	✓	✓
	Windows 10 IoT Core Services	✓	-
Integration	API Management	✓	✓
	Azure Logic Apps	✓	✓
	Service Bus	✓	✓
Identity	Azure Active Directory	✓	✓
	Azure Active Directory B2C	✓	-
	Azure Active Directory Domain Services	✓	✓
	Azure Information Protection	✓	✓
Management and Governance	Application Change Analysis	✓	-
	Automation	✓	✓
	Azure Advisor	✓	✓
	Azure Blueprints	✓	✓
	Azure Lighthouse	✓	✓
	Azure Managed Applications	✓	✓
	Azure Migrate	✓	✓
	Azure Monitor	✓	✓
	Azure Policy	✓	✓
	Azure Resource Graph	✓	✓
	Azure Resource Manager (ARM)	✓	✓
	Azure Signup Portal	✓	✓
	Cost Management	✓	✓
	Cloud Shell	✓	✓
	Microsoft Azure Portal	✓	✓
	Microsoft Purview	✓	-

Product Category Offering / Service		Cloud Environment Scope	
		Azure	Azure Government
	Azure Quotas	✓	✓
Security	Azure Confidential Computing	✓	-
	Azure Dedicated HSM	✓	✓
	Azure Payment HSM	✓	-
	Microsoft Defender for Cloud	✓	✓
	Microsoft Sentinel	✓	✓
	Customer Lockbox for Microsoft Azure	✓	✓
	Key Vault	✓	✓
	Microsoft Azure Attestation	✓	-
	Multi-Factor Authentication	✓	✓
Media	Azure Media Services	✓	✓
Web	Azure Cognitive Search	✓	✓
	Azure Fluid Relay	✓	-
	Azure Maps	✓	✓
	Azure SignalR Service	✓	✓
	Azure Spring Apps	✓	-
	Azure Web PubSub	✓	✓
Mixed Reality	Azure Remote Rendering	✓	-
	Azure Spatial Anchors	✓	-
Internal Supporting Services ⁶		✓	✓

⁶ Azure Government scope boundary for internal services: Asimov Event Forwarder, Autopilot Security, AzCP Platform, Azure Diagnostic Services, Azure Security Monitoring (ASM SLAM), Azure Service Health, Azure Stack Bridge, Azure Stack Edge Service, Azure System Lockdown, Azure Watson, Azure AI Services: Container Platform, CoreWAN, dSCM, dSMS, dSTS, Dynamics 365 Integrator App, Fabric Controller Fundamental Services, Fabric Network Devices, Gateway Manager, Geneva Actions, Geneva Analytics Orchestration, Geneva Warm Path, Interflow, JIT, MDM, MEE Privacy Service, Microsoft Email Orchestrator, MSaaS File Management (DTM V2), MSFT.RR DNS, Network Billing, OneBranch Release, OneDeploy Deployment Infrastructure (DE), OneDS Collector, OneIdentity, PF-FC, Pilotfish, Unified Remote Scanning (URSA), Vulnerability Scanning & Analytics, WaNetMon, Windows Azure Jumpbox, and Workflow. The coverage period for internal services for both Azure and Azure Government is July 1, 2022 through June 30, 2023 except for those specified with shorter coverage periods in the Internal Supporting Services subsection herein.

Offering	Cloud Environment Scope	
	Azure	Azure Government
Microsoft Online Services		
Appsource	✓	-
Dynamics 365 Customer Voice	✓	-
Intelligent Recommendations	✓	-
Microsoft Defender for Cloud Apps	✓	✓
Microsoft Defender for Endpoint	✓	✓
Microsoft Defender for Identity	✓	✓
Microsoft Graph	✓	✓
Microsoft Intune	✓	✓
Microsoft Managed Desktop	✓	-
Microsoft Stream	✓	✓
Endpoint Attack Notifications	✓	-
Nomination Portal	✓	✓
Power Apps	✓	✓
Power Automate	✓	✓
Power BI	✓	✓
Power Virtual Agents	✓	✓
Windows Update for Business reports	✓	-

Offering	Cloud Environment Scope	
	Azure	Azure Government
Microsoft Dynamics 365		
Chat for Dynamics 365	✓	✓
Dataverse	✓	✓
Dynamics 365 AI Customer Insights	✓	✓
Dynamics 365 Athena - CDS to Azure Data Lake	✓	✓

Offering	Cloud Environment Scope	
	Azure	Azure Government
Dynamics 365 Business Central	✓	-
Dynamics 365 Business Q&A	✓	-
Dynamics 365 Commerce	✓	-
Dynamics 365 Customer Insights Engagement Insights	✓	-
Dynamics 365 Customer Service	✓	✓
Dynamics 365 Field Service	✓	✓
Dynamics 365 Finance	✓	✓
Dynamics 365 Fraud Protection	✓	-
Dynamics 365 Guides	✓	-
Dynamics 365 Human Resources	✓	-
Dynamics 365 Intelligent Order Management	✓	-
Dynamics 365 Marketing	✓	-
Dynamics 365 Project Operations	✓	-
Dynamics 365 Remote Assist	✓	-
Dynamics 365 Retail	✓	-
Dynamics 365 Sales	✓	✓
Dynamics 365 Sales Insights	✓	-
Dynamics 365 Supply Chain Management	✓	-
Dynamics 365 Talent Attract & Onboard ⁵	✓	-
Power Pages	✓	✓

Offering	Cloud Environment Scope	
	Azure	Azure Government
Microsoft Cloud for Financial Services		
Unified Customer Profile	✓	-
Collaboration Manager	✓	-
Customer Onboarding	✓	-

Regions Covered by this Report

Azure production infrastructure is located in globally distributed datacenters. These datacenters across multiple regions deliver the core physical infrastructure that includes physical hardware asset management, security, data protection, networking services. These datacenters are managed, monitored, and operated by Microsoft operations staff delivering online services with 24x7 continuity. The purpose-built facilities are part of a network of datacenters that provide mission critical services to Azure and other Online Services. The datacenters in scope for the purposes of this report are:

Azure Regions

Americas

- West US
- West US 2
- West US 3
- West Central US
- Central US
- USGOV Iowa
- North Central US
- USGOV Arizona
- South Central US
- USGOV Texas
- East US
- East US 2
- USGOV Virginia
- USGOV Wyoming
- Canada East
- Canada Central
- Brazil South
- Brazil Southeast

APAC

- Australia East
- Australia Southeast
- Australia Central
- Australia Central 2
- West India
- Central India
- Jio India West
- Jio India Central
- South India
- East Asia
- Japan West
- Japan East
- Southeast Asia
- Korea South
- Korea Central

EMEA

- West Europe
- North Europe
- UK South
- UK West
- France Central
- France South
- Germany North
- Germany West Central
- Switzerland West
- Switzerland North
- Norway East
- Norway West
- Qatar Central
- Sweden Central
- Sweden South
- South Africa North
- South Africa West
- UAE Central
- UAE North

In addition to the datacenters included in the Azure regions listed above, there are datacenters outside of those regions which are included in the scope of the examination and are supporting Office 365 services. Note that the Office 365 services are not included in the scope of the examination.

In addition to datacenter, network, and personnel security practices, Azure also incorporates security practices at the application and platform layers to enhance security for application development and service administration.

Edge Sites

- Ashburn, VA (ASH⁷)
 - Athens, Greece (ATH01)
 - Atlanta, GA (ATA)
 - Auckland, New Zealand (AKL30)
 - Bangkok, Thailand (BKK30)
 - Barcelona, Spain (BCN30)
 - Barueri, Brazil (GRU30)
 - Berlin, Germany (BER30)
 - Bogota, Colombia (BOG30)
 - Boston, MA (BOS31⁷)
 - Brisbane, Australia (BNE01)
 - Brussels, Belgium (BRU30)
 - Bucharest, Romania (BUH01)
 - Budapest, Hungary (BUD01)
 - Buenos Aires, Argentina (BUE30)
 - Busan, South Korea (PUS03)
 - Cairo, Egypt (CAI30)
 - Cape Town, South Africa (CPT02)
 - Chicago, IL (CHG, CHI30)
 - Cincinnati, OH (CVG30)
 - Copenhagen, Denmark (CPH30)
 - Dallas, TX (DAL⁷, DFW30)
 - Detroit, MI (DTT30⁸)
 - Doha, Qatar (DOH30/31)
 - Dubai, United Arab Emirates (DXB30)
 - Dusseldorf, Germany (DUS30)
 - Frankfurt, Germany (FRA/31)
 - Geneva, Switzerland (GVA30)
 - Helsinki, Finland (HEL02)
 - Ho Chi Minh City, Vietnam (SGN30)
 - Hong Kong (HKB, HKG30)
 - Honolulu, HI (HNL01)
 - Houston, TX (HOU01)
 - Hyderabad, India (HYD30)
 - Istanbul, Turkey (IST30)
 - Jakarta, Indonesia (JKT30)
 - Jacksonville, FL (JAX30)
 - Johannesburg, South Africa (JNB02)
 - Kuala Lumpur, Malaysia (KUL02/30)
 - Las Vegas, NV (LAS30)
 - Luanda, Angola (LAD30)
 - Lisbon, Portugal (LIS01)
 - London, United Kingdom (LON04, LTS)
 - Los Angeles, CA (LAX)
 - Lagos, Nigeria (LOS30)
 - Madrid, Spain (MAD30)
 - Manchester, United Kingdom (MAN30/31⁸)
 - Manila, Philippines (MNL30)
 - Memphis, TN (MEM30)
 - Miami, FL (MIA)
 - Milan, Italy (MIL30)
 - Minneapolis, MN (MSP30)
 - Montreal, Canada (YMQ01)
 - Mumbai, India (BOM02)
 - Munich, Germany (MUC30)
 - Nairobi, Kenya (NBO30)
 - Nashville, TN (BNA30)
 - New Delhi, India (DEL01)
 - New York City, NY (NYC)
 - Newark, NJ (EWR30)
 - Osaka, Japan (OSA30/31)
 - Oslo, Norway (OSL30)
 - Palo Alto, CA (PAO)
 - Paris, France (PAR02/PRA)
 - Perth, Australia (PER01⁷/30⁷)
 - Philadelphia, PA (PHL30)
 - Phoenix, AZ (PHX31)
 - Portland, OR (PDX31)
 - Prague, Czech Republic (PRG01)
 - Pune, India (PNQ30)
 - Queretaro, Mexico (MEX30/31)
 - Rabat, Morocco (RBA30)
 - Rio de Janeiro (RIO02/03)
 - Rome, Italy (ROM30)
 - Sao Paulo, Brazil (SAO31)
 - Salt Lake City, UT (SLC31)
 - San Diego, CA (SAN30⁷)
 - San Jose, CA (SJC)
 - Santiago, Chile (SCL30)
 - Seattle, WA (WST, STB)
 - Seoul, South Korea (SLA)
 - Singapore (SGE, SIN30, SG1)
 - Sofia, Bulgaria (SOF01)
 - Stockholm, Sweden (STO)
 - Taipei, Taiwan (TPE30/31)
 - Tampa, FL (TPA30⁷)
 - Tel Aviv, Israel (TLV30)
 - Teterboro, NJ (TEB31)
 - Tokyo, Japan (TYA/TYB)
 - Toronto, Canada (YTO01/30)
 - Vancouver, Canada (YVR30)
 - Warsaw, Poland (WAW01/30⁸)
 - Zagreb, Croatia (ZAG30)
 - Zurich, Switzerland (ZRH)
-

⁷ Examination period for this edge site was from July 1, 2022 to September 30, 2022.

⁸ Examination period for this edge site was from October 1, 2022 to March 31, 2023.

Control Environment

Integrity and Ethical Values

Corporate governance at Microsoft starts with an independent Board of Directors that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span across the company. Corporate governance at Microsoft serves several purposes:

1. To establish and preserve management accountability to Microsoft's owners by appropriately distributing rights and responsibilities among Microsoft Board members, managers, and shareholders
2. To provide a structure through which management and the Board set and attain objectives and monitor performance
3. To strengthen and safeguard a culture of business integrity and responsible business practices
4. To encourage efficient use of resources and to require accountability for stewardship of these resources

Further information about Microsoft's general corporate governance is available on the Microsoft public website.

Microsoft Standards of Business Conduct

The Microsoft Standards of Business Conduct (SBC) reflect a commitment to ethical business practices and regulatory compliance. They summarize the principles and policies that guide Microsoft's business activities and provide information about Microsoft's Business Conduct and Compliance Program. SBC was developed in full consideration of Sarbanes-Oxley Act (SOX) and proposed NASDAQ listing requirements related to codes of conduct. Additional information about Microsoft's SBC is available on the Microsoft public website.

Training

Annual SBC training is mandatory for all Microsoft employees and contingent staff. The SBC training includes information about Microsoft corporate policies for conducting business while conforming to applicable laws and regulations. It reinforces the need for employees to work with integrity and to comply with the laws of the countries in which Microsoft operates. It also guides employees and contingent staff on the processes and channels available to report possible violations or to ask questions.

Accountability

All Microsoft and contingent staff are accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy, and any applicable supporting procedures. Individuals not employed by Microsoft, but allowed to access, manage, or process information assets of the Azure environment and datacenters are also accountable for understanding and adhering to the guidance contained in the Security Policy and standards.

Commitment to Competence

Microsoft hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background skills needed to perform the job, and personal qualifications desired. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and make an appropriate hiring decision.

Microsoft employees create individual Core Priorities that align with those of their manager, organization, and Microsoft, and are supported with customer-centric actions and measures so that everyone is working toward the same overarching vision. These Core Priorities are established when an employee is hired, and then updated

during one-on-one Connect meetings with their manager. The primary focus of the Connect meetings is to assess employee performance against their priorities and to agree on an updated list of priorities going forward.

Microsoft's Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers.

Internal Communication

Responsibilities around internal controls are communicated broadly through Monthly Controller calls, All Hands Meetings run by the Chief Financial Officer (CFO), and email updates sent / conference calls held by the Financial Compliance Group with the Sarbanes-Oxley extended project team. Responsibilities for compliance with policies are outlined in the SBC training.

Compliance & Ethics - Board of Directors and Senior Leadership

Compliance & Ethics designs and provides reports to the Board of Directors on compliance matters. They also organize annual meetings with the Senior Leadership Team (SLT) for their compliance review.

Internal Audit Department

Microsoft has an Internal Audit (IA) function that reports directly to the Audit Committee (AC) of the Board of Directors, which is constituted solely of independent directors. IA has a formal charter that is reviewed by the AC and management. Responsibilities of IA include performing audits and reporting issues and recommendations to management and the AC.

Audit Committee

The AC charter and responsibilities are on Microsoft's website. The AC meets privately on a quarterly basis with Microsoft's external auditors and IA. The agendas for the quarterly AC meetings are found in the AC Responsibilities Calendar sent out with the charter. In addition, the AC influences the company through the IA function. The AC reviews the scope of internal audit and assists in the process of identifying and resolving any issues. Lastly, the AC monitors itself by completing an annual self-evaluation.

Risk Assessment

Practices for Identification of Risk

The Microsoft Enterprise Risk Management (ERM) team provides management and accountability of Microsoft Corporate's short- and long-term risks. ERM collaborates with Internal Audit, the Financial Compliance Group, Operations, and Legal and Compliance groups to perform a formal risk assessment. These risk assessments include risks in financial reporting, fraud, and compliance with laws.

Internal Audit - Fraud Risks

IA and the Financial Integrity Unit (FIU) are responsible for identifying fraud risks across Microsoft. The FIU performs procedures for the detection, investigation, and prevention of financial fraud impacting Microsoft worldwide. Fraud and abuse that are uncovered are reported to the Disclosure Committee. The FIU provides both a reactive and proactive response to allegations of fraud and abuse. The FIU uses a case management system that is also used by the Director of Compliance to track cases and related metrics. The FIU interacts with Microsoft management, Corporate, External, and Legal Affairs (CELA), Human Resource (HR), Finance, Procurement, and others to determine specific fraud risks and responses.

Periodic Risk Assessment

IA and other groups within the company perform a periodic risk assessment. The assessment is reviewed by senior management.

IA specialization area leaders determine high-priority risks across the company, including risks related to financial reporting, operational business process, and systems controls. Control failures are also assessed to determine whether they give rise to additional risks.

Compliance & Ethics / Internal Audit / Risk Management - Risk Responsibility

The responsibility for risk is distributed throughout the organization based on the individual group's services. Compliance & Ethics, IA, and the ERM team work together to represent enterprise risk management. Through quarter and year-end reviews, the CFO, and Corporate Controller (and respective groups) review the disclosures and issues that may have arisen.

Monitoring

Security and Compliance Monitoring

Azure and the datacenters maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

Compliance & Ethics - Business Conduct Hotline

There is a confidential and anonymous Business Conduct Hotline available for employees to report issues. The hotline is accessible 24x7 through email, phone, fax, and mail. The individual may also send a letter or fax reporting the concern to Microsoft's Compliance & Ethics - Business & Regulatory Investigations team.

Employees are instructed that it is their duty to promptly report any concerns of suspected or known violations of the Code of Professional Conduct, the SBC, or other Microsoft policies or guidelines. The procedures to be followed for such a report are outlined in the SBC and the Whistle Blowing Reporting Procedure and Guidelines in the Employee Handbook. Employees are also encouraged to communicate the issue to their manager, their manager's manager, their CELA contact, their HR contact, or the Compliance Office.

Internal Audit

Microsoft's IA department provides support to management across the company by independently and objectively assessing whether the objectives of management are adequately performed, and by facilitating process improvements, and the adoption of business practices, policies, and controls governing worldwide operations.

Information and Communication

An annual process exists to set objectives and commitments among all executives and is rolled down to employees. These commitments and objectives are filtered down to team members through the annual and midyear review process.

Office of the CFO - Communications External to the Company

CFO communications outside the company occur throughout the year and, where appropriate, these external communications include a discussion of the company's attitude toward sound internal controls. The Office of the CFO is responsible for a number of communications outside the company, including Quarterly Earnings Release, Financial Analyst meetings, customer visits, external conferences, and external publications.

Data

Customers upload data for storage or processing within the services or applications that are hosted on the cloud services platform. In addition, certain types of data are provided by the customers or generated on the customer's behalf to enable the usage of the cloud services. Microsoft only uses customer data in order to support the provisioning of the services subscribed to by the customers in accordance with the Service Level Agreements (SLAs). The customer provided data are broadly classified into the following data types:

1. **Access Control Data** is data used to manage access to administrative roles or sensitive functions.
2. **Customer Content** is the data, information and code that Microsoft internal employees, and non-Microsoft personnel (if present) provide to, transfer in, store in or process in a Microsoft Online Service or product.
3. **End User Identifiable Information (EUII)** is data that directly identifies or could be used to identify the authenticated user of a Microsoft service. EUII does not extend to other personal information found in Customer Content.
4. **Support Data** is data provided to Microsoft and generated by Microsoft as part of support activities.
5. **Feedback** is data provided as part of a review or feedback for one of Microsoft's products and services that includes personal data.
6. **Account Data** is information about payment instruments. This type of data is not stored in the Azure platform.
7. **Public Personal Data** is publicly available personal information that Microsoft obtains from external sources.
8. **End User Pseudonymous Identifiers (EUPI)** are identifiers created by Microsoft, tied to the user of a Microsoft service.
9. **Managed Service Data** is all data provided to Microsoft by the Managed Service customer and / or the Managed Service personnel as part of a Managed Service engagement.
10. **Organization Identifiable Information (OII)** is data that can be used to identify a particular tenant / Azure subscription / deployment / organization (generally configuration or usage data) and is not linkable to a user.
11. **System Metadata** is data generated in the course of running the service, not linkable to a user or tenant. It does not contain Access Control Data, Customer Content, EUII, Support Data, Account Data, Public Personal Data, EUPI, or OII.
12. **Public Non-Personal Data** is publicly available information that Microsoft obtains from external sources. It does not contain Public Personal Data.

Data Ownership

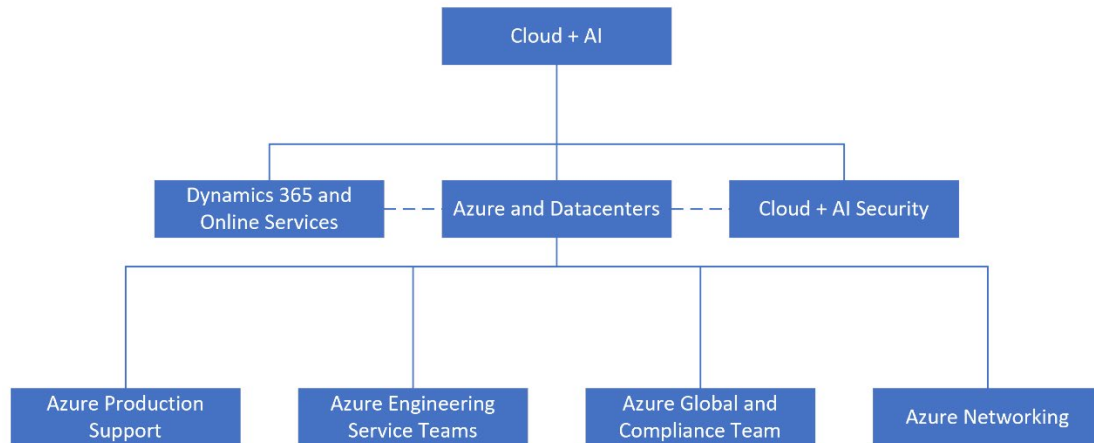
Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information entered into Azure. Azure's Agreement states, "Customers are solely responsible for the content of all Customer Data. Customers will secure and maintain all rights in Customer Data necessary for Azure to provide the Online Services to them without violating the rights of any third party or otherwise obligating Microsoft to them or to any third party. Microsoft does not and will not assume any obligations with respect to Customer Data or to their use of the Product other than as expressly set forth in the Agreement or as required by applicable law."

Applicable Data Elements

For the purposes of this report, Microsoft has implemented controls to protect the data elements specifically covered under Customer Content and Access Control Data.

People

Azure is comprised and supported by the following groups who are responsible for the delivery and management of Azure services:



Online Services

Online Services teams manage the service lifecycle of the finished SaaS services that leverage the underlying Azure platform and datacenter infrastructure. They are responsible for the development of new features, operational support, and escalations.

Cloud + AI Security

The Cloud + AI Security team works to make Azure a secure and compliant cloud platform by building common security technologies, tools, processes, and best practices. The Cloud + AI Security team is involved in the review of deployments and enhancements of Azure services to facilitate security considerations at every level of the Security Development Lifecycle (SDL). They also perform security reviews and provide security guidance for the datacenters. This team consists of personnel responsible for:

- Security Development Lifecycle
- Security incident response
- Driving security functionality within service development work

Azure Production Support

The Azure Production Support team is responsible for build-out, deployment and management of Azure services. This team consists of the following:

- **Azure Live Site** - Monitors and supports the Azure platform; proactively addresses potential platform issues; and reacts to incidents and support requests
- **Azure Deployment Engineering** - Builds out new capacity for the Azure platform; and deploys platform and product releases through the release pipeline
- **Azure Customer Support** - Provides support to individual customers and multinational enterprises from basic break-fix support to rapid response support for mission critical applications

Azure Engineering Service Teams

The Azure Engineering Service teams manage the service lifecycle. Their responsibilities include:

- Development of new services
- Serving as an escalation point for support
- Providing operational support for existing services (DevOps model)

The team includes personnel from the Development, Test and Program Management (PM) disciplines for design, development, and testing of services, and providing technical support as needed.

Global Ecosystem and Compliance Team

The Global Ecosystem and Compliance team is responsible for developing, maintaining and monitoring the Information Security (IS) program including the ongoing risk assessment process.

As part of managing compliance adherence, the team drives related features within the Azure product families. This team consists of personnel responsible for:

- Training
- Privacy
- Risk assessment
- Internal and external audit coordination

Networking

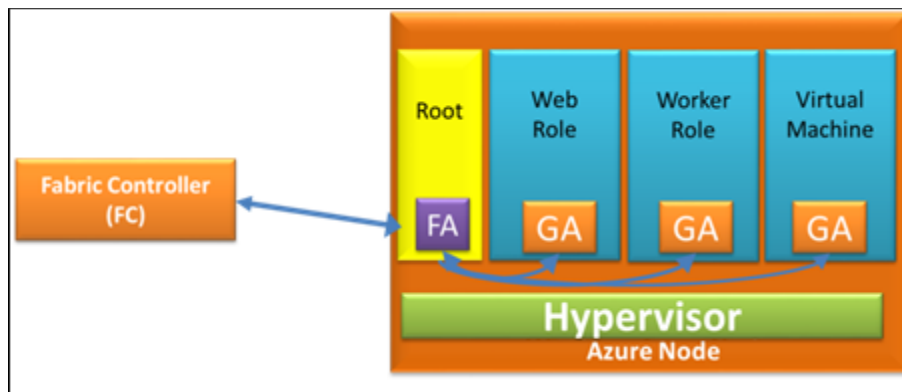
The Networking team is responsible for implementing, monitoring and maintaining the Microsoft network. This team consists of personnel responsible for:

- Network configuration and access management
- Network problem management
- Network capacity management

Azure Environment

Azure is developed and managed by the Azure team, and provides a cloud platform based on machine [virtualization](#). This means that customer code - whether it's deployed in a PaaS Worker Role or an IaaS Virtual Machine - executes in a Windows Server Hyper-V virtual machine. Every physical node in Azure has one or more virtual machines, also called instances, that are scheduled on physical CPU cores, are assigned dedicated RAM, and have controlled access to local disk and network I/O.

On each Azure node, there is a Hypervisor that runs directly over the hardware and divides a node into a variable number of Guest Virtual Machines (VMs). Each node also has one special Root VM, which runs the Host Operating System (OS), as shown in figure below. Fabric Agents (FAs) on Root VMs are used to manage Guest Agents (GAs) within Guest VMs. Isolation of the Root VM from the Guest VMs and the Guest VMs from one another is a key concept in Azure security architecture.



Fabric Controller Lifecycle Management

In Azure, VMs (nodes) run on groups of physical servers known as “clusters”, of approximately 1,000 machines. Each cluster is independently managed by a scaled-out and redundant platform Fabric Controller (FC) software component.

Each FC manages the lifecycle of VMs and applications running in its cluster, including provisioning and monitoring the health of the hardware under its control. The FC executes both automatic operations, like healing VM instances to healthy servers when it determines that the original server has failed, as well as application-management operations like deploying, updating, reimaging and scaling out applications. Dividing the datacenter into clusters isolates faults at the FC level, preventing certain classes of errors from affecting servers beyond the cluster in which they occur. FCs that serve a particular Azure cluster are grouped into FC Clusters.

FC Managed Operating Systems

An Azure OS base image Virtual Hard Disk (VHD) is deployed on all Host, Native, and Guest VMs in the Azure production environment. The three types of FC managed OS images are:

1. **Host OS:** Host OS is a customized version of the Windows OS that runs on Host Machine Root VMs
2. **Native OS:** Native OS runs on Azure native tenants such as the FC itself, Azure Storage and Azure Load Balancer that do not have any hypervisor
3. **Guest OS:** Guest OS runs on Guest VMs (for IaaS, FC will run customer provided images on a VHD)

The Host OS and Native OS are OS images that run on physical servers and native tenants and host the Fabric Agent and other Host components. The Guest OS provides the most up-to-date runtime environment for Azure customers and can be automatically upgraded with new OS releases or manually upgraded based on customer preference.

Software Development Kits

Azure allows customers to create applications in many development languages. Microsoft provides language-specific Software Development Kits (SDKs) for .NET, Java, PHP, Ruby, Node.js and others. In addition, there is a general Azure SDK that provides basic support for any language, such as C++ or Python. These SDKs can be used with development tools such as Visual Studio and Eclipse.

These SDKs also support creating applications running outside the cloud that use Azure services. For example, a customer can build an application running on a Host that relies on Azure Blob Storage, or create a tool that automatically deploys Azure applications through the platform’s management interface.

Azure Services and Offerings

Azure services and offerings are grouped into categories discussed below. A complete list of Azure services and offerings available to customers is provided in the [Azure Service Directory](#). Brief descriptions for each of the customer-facing services and offerings in scope for this report are provided below. Customers should consult extensive online documentation for additional information.

Compute

[Azure Arc](#): Azure Arc allows customers to manage, monitor and govern machines running on-premises or in other clouds, from Azure.

[App Service](#): App Service enables customers to quickly build, deploy, and scale enterprise-grade web, mobile, and applications and programming interface (API) apps that can run on a number of different platforms.

- [App Service: API Apps](#): API Apps enables customers to build and consume Cloud APIs. Customers can connect their preferred version control system to their API Apps, and automatically deploy commits, making code changes.
- [App Service: Mobile Apps](#): Mobile Apps allows customers to accelerate mobile application development by providing a turnkey way to structure storage, authenticate users, and send push notifications. Mobile Apps allows customers to build connected applications for any platform and deliver a consistent experience across devices.
- [App Service: Web Apps](#): Web Apps offers secure and flexible development, deployment and scaling options for web applications of any size. Web Apps enables provisioning a production web application in minutes using a variety of methods including the Azure Portal, PowerShell scripts running on Windows, Command Line Interface tools running on any OS, source code control driven deployments, as well as from within the Visual Studio Integrated Development Environment (IDE).
- [Azure App Service Static Web Apps](#): Static Web Apps offers streamlined full-stack development from source code to global high availability. It allows customers accelerated app development with a static front end and dynamic back end powered by serverless APIs. Customers experience high productivity with a tailored local development experience, GitHub native workflows to build and deploy apps, and unified hosting and management in the cloud.

[Azure Cloud Services](#): Azure Cloud Services is a PaaS service designed to support applications that are scalable, reliable, and inexpensive to operate. Azure Cloud Services is hosted on virtual machines. However, customers have more control over the VMs. Customers can install their own software on VMs that use Azure Cloud Services and access them remotely. It removes the need to manage server infrastructure and lets customers build, deploy, and manage modern applications with web and worker roles.

[Azure Functions](#): Azure Functions is a serverless compute service that lets customers run event-triggered code without having to explicitly provision or manage infrastructure. Azure Functions is an event driven, compute-on-demand experience. Customers can leverage Azure Functions to build Hypertext Transfer Protocol (HTTP) endpoints accessible by mobile and Internet of Things (IoT) devices.

[Azure Service Fabric](#): Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers. It is a micro-services platform used to build scalable managed applications for the cloud. Azure Service Fabric addresses significant challenges in developing and managing cloud applications by allowing developers and administrators to shift focus from infrastructure maintenance to implementation of mission-critical, demanding workloads.

[Azure VM Image Builder](#): Azure VM Image Builder is an Azure Resource Provider service that allows customers to create custom virtual machine images.

[Azure VMware Solution](#): Azure VMware Solution delivers a comprehensive VMware environment in Azure allowing customers to run native VMware workloads on Azure. Azure VMware Solution allows customers to

seamlessly run, manage and secure applications across VMware environments and Microsoft Azure with a common operating framework.

Batch: Batch runs large-scale parallel applications and High-Performance Computing (HPC) workloads efficiently in the cloud. It allows customers to schedule compute-intensive tasks and dynamically adjust resources for their solution without managing the infrastructure. Customers can use Batch to scale out parallel workloads, manage the execution of tasks in a queue, and cloud-enable applications to offload compute jobs to the cloud.

Machine Configuration: Machine Configuration provides management and configuration capabilities to Azure compute resources in Azure and Arc VMs. Machine Configuration uses the Azure policy to audit the internal configuration of a VM's OS, deployed applications, and the environment configuration. Machine Configuration is a digital security and risk engineering DevOps Kit baseline control and helps audit VM configurations.

Planned Maintenance: Planned Maintenance is responsible for the roll out of planned maintenance activities to the nodes and VMs in Azure.

Virtual Machines: Virtual Machines is one of the several types of on-demand, scalable computing resources that Azure offers. Virtual Machines, which includes Azure Reserved Virtual Machine Instances, lets customers deploy a Windows Server or a Linux image in the cloud. Customers can select images from a marketplace or use their own customized images. It gives customers the flexibility of virtualization without having to buy and maintain the physical hardware that runs it.

Virtual Machine Scale Sets: Virtual Machine Scale Sets service lets customers create and manage a group of identical, load balanced, and autoscaling VMs. It makes it possible to build highly scalable applications by allowing customers to deploy and manage identical VMs as a set. VM Scale sets are built on the Azure Resource Manager deployment model, are fully integrated with Azure load balancing and autoscaling, and support Windows and / or Linux custom images, and extensions.

Azure Virtual Desktop: Azure Virtual Desktop is a virtualization management service running on Azure that provisions and manages connections to virtual desktops and apps on Windows 7, Windows 10, Windows Server 2012 R2+ in single or multi-session environments. It allows users to set up a scalable and flexible environment as well as connect, deploy to, and manage virtual desktops.

Containers

Azure Arc Enabled Kubernetes: Azure Arc Enabled Kubernetes allows customers (cluster operators) to use Azure as their single control plane for connecting, configuring and governing their Kubernetes clusters spread out across other public clouds and on-premise environments.

Azure Container Apps: Azure Container Apps is a fully managed environment that enables customers to run microservices and containerized applications on a serverless platform. Common uses of Azure Container Apps include deploying API endpoints, hosting background processing applications, handling event-driven processing, and running microservices.

Azure Container Registry: Azure Container Registry allows customers the ability to store images for all types of container deployments including DC / OS, Docker Swarm, Kubernetes, and Azure services such as App Service, Batch, Azure Service Fabric, and others. Developers can manage the configuration of apps isolated from the configuration of the hosting environment. Azure Container Registry reduces network latency and eliminates ingress / egress charges by keeping Docker registries in the same datacenters as customers' deployments. It provides local, network-close storage of container images within subscriptions, and full control over access and image names.

Azure Kubernetes Configuration Management: Azure Kubernetes Configuration Management allows customers (cluster operators) to use GitOps to manage configuration on various Kubernetes clusters - Azure Arc connected clusters, AKS clusters, and eventually other cluster types like Azure Red Hat OpenShift (ARO).

[Azure Kubernetes Service \(AKS\)](#): Azure Kubernetes Service is an enterprise ready managed service that allows customers to run Open source Kubernetes on Azure without having to manage it on their own. It also includes the functionality of Azure Container service (ACS), which was retired in calendar year Q1 2020. ACS was a container hosting environment which provided users the choice of container orchestration platforms such as Mesosphere DC/OS and Docker Swarm. AKS makes deploying and managing containerized applications easy. It offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience, and enterprise-grade security and governance. AKS unites the customer development and operations teams on a single platform to rapidly build, deliver, and scale applications with confidence.

[Azure Red Hat OpenShift](#): Azure Red Hat OpenShift offering provides flexible, self-service deployment of fully managed OpenShift clusters. It helps customers maintain regulatory compliance and focus on their application development, while the master, infrastructure, and application nodes are patched, updated, and monitored by both Microsoft and Red Hat.

[Container Instances](#): Container Instances enables the creation of containers as first-class objects in Azure, without requiring VM management and without enforcing any prescriptive application model. Container Instances is a solution for any scenario that can operate in isolated containers, without orchestration. Customer can run event-driven applications, quickly deploy from their container development pipelines, and run data processing and build jobs.

Networking

[Application Gateway](#): Application Gateway is a web traffic load balancer that enables customers to manage traffic to their web applications. It is an Azure-managed layer-7 solution providing HTTP load balancing, Web Application Firewall (WAF), Transport Layer Security (TLS) termination service, and session-based cookie affinity to Internet-facing or internal web applications.

[Azure Bastion](#): Azure Bastion is a managed PaaS service that provides secure and seamless Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to customer's virtual machines directly through the Azure Portal. Azure Bastion is provisioned directly in the customer Virtual Network (VNet) and supports all VMs in their VNet using SSL without any exposure through public IP addresses.

[Azure DDoS Protection](#): Azure DDoS Protection is a fully automated solution aimed primarily at protecting resources against Distributed Denial of Service (DDoS) attacks. Azure DDoS Protection helps prevent service interruptions by eliminating harmful volumetric traffic flows.

[Azure DNS](#): Azure DNS is a hosting service for Domain Name System (DNS) domains that provides name resolution by using Microsoft Azure infrastructure. Azure DNS lets customers host their DNS domains alongside their Azure apps and manage DNS records by using the same credentials, APIs, tools, and billing as their other Azure services.

[Azure ExpressRoute](#): Azure ExpressRoute lets customers create private connections between Azure datacenters and customer's infrastructure located on-premises or in a colocation environment. ExpressRoute connections do not go over the public Internet, and offer more reliability, faster speeds, and lower latencies than typical Internet connections.

[Azure Firewall](#): Azure Firewall is a managed cloud-based network security service that protects Azure virtual network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. Customers can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for virtual network resources allowing outside firewalls to identify traffic originating from a virtual network. This service is fully integrated with Azure Monitor Essentials for logging and analytics purposes.

[Azure Firewall Manager](#): Azure Firewall Manager is a security management service that provides central security policy and route management for cloud-based security perimeters. Azure Firewall Manager simplifies central configuration and management of rules for multiple Azure Firewall instances, across Azure regions and

subscriptions. This allows customers to automate Azure Firewall deployment to multiple secured virtual hubs and integrates with trusted security partner solutions for advanced services.

[**Azure Front Door:**](#) Azure Front Door (AFD) is Microsoft's highly available and scalable Web Application Acceleration Platform, Global HTTP Load Balancer, Application Protection and Azure Content Delivery Network. AFD enables customers to build, operate and scale out their dynamic web application and static content. AFD provides customers' application with end-user performance, unified regional / stamp maintenance automation, Business Continuity and Disaster Recovery (BCDR) automation, unified client / user information, caching and service insights.

[**Azure Internet Analyzer:**](#) Azure Internet Analyzer is a client-side measurement platform that tests how changes to customer's networking infrastructure impact their client's / end-user's performance. Internet Analyzer uses a small JavaScript client embedded in the customer's web application to measure the latency from their end-users to customer selected set of network destinations (endpoints). Internet Analyzer allows customers to set up multiple side-by-side tests, allowing to evaluate a variety of scenarios as their infrastructure and needs evolve. It provides custom and preconfigured endpoints, providing a customer both the convenience and flexibility to make trusted performance decisions for their end-users.

[**Azure Private Link:**](#) Azure Private Link provides private connectivity from a virtual network to Azure PaaS, customer-owned, or Microsoft partner services. It simplifies the network architecture and secures the connection between endpoints in Azure by eliminating data exposure to the public Internet.

[**Azure Route Server:**](#) Azure Route Server enables the customer's network appliances to exchange route information with Azure virtual networks dynamically. It allows customers to exchange routing information directly through Border Gateway Protocol (BGP) routing protocol between any Network Virtual Appliances (NVA) that supports the BGP routing protocol and the Azure Software Defined Network (SDN) in the Azure Virtual Network (VNET) without the need to manually configure or maintain route tables.

[**Azure Web Application Firewall:**](#) Azure Web Application Firewall helps protect customer's web apps from malicious attacks and top 10 Open Web Application Security Project (OWASP) security vulnerabilities, such as SQL injection and cross-site scripting. Cloud-native Azure Web Application Firewall service deploys in minutes and offers customized rules that meet the customer's web app security requirements.

[**Azure Content Delivery Network:**](#) Azure Content Delivery Network (CDN) sends audio, video, applications, images, and other files faster and more reliably to customers by using the servers that are closest to each user. This dramatically increases speed and availability. Due to its distributed global scale, CDN can handle sudden traffic spikes and heavy loads without new infrastructure costs or capacity worries. CDN is built on a highly scalable, reverse-proxy architecture with sophisticated DDoS identification and mitigation technologies. Customers can choose to use Azure CDN from Verizon or Akamai partners. Verizon and Akamai are not covered in this SOC report.

[**IP Services:**](#) IP Services allows Internet resources to communicate inbound to Azure resources, as well as providing a predictable method for communicating outbound to the Internet and other public-facing Azure services. Customers can associate IP Services addresses to virtual machine network interfaces, public load balancers, VPN gateways, and other resources.

[**Azure Load Balancer:**](#) Azure Load Balancer distributes Internet and private network traffic among healthy service instances in cloud services or virtual machines. It lets customers achieve greater reliability and seamlessly add more capacity to their applications.

[**Microsoft Azure Peering Service:**](#) Microsoft Azure Peering Service is a networking service that enhances customer connectivity to Microsoft cloud services such as Microsoft 365, Dynamics 365, SaaS services, Azure, or any Microsoft services accessible via the public Internet. Microsoft has partnered with Internet Service Providers (ISPs), Internet Exchange Partners, and Software-Defined Cloud Interconnect (SDCI) providers worldwide to provide reliable and high-performing public connectivity with optimal routing from the customer to the Microsoft network.

[Network Watcher](#): Network Watcher enables customers to monitor and diagnose conditions at a network scenario level. Network diagnostic and visualization tools available with Network Watcher allow customers to take packet captures on a VM, help them understand if an IP flow is allowed or denied on their Virtual Machine, find where their packet will be routed from a VM and gain insights to their network topology.

[Traffic Manager](#): Traffic Manager is a DNS-based traffic load balancer that enables customers to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints.

[Virtual Network](#): Virtual Network lets customers create private networks in the cloud with full control over IP addresses, DNS servers, security rules, and traffic flows. Customers can securely connect a virtual network to on-premises networks by using a Virtual Private Network (VPN) tunnel, or connect privately by using the Azure ExpressRoute service.

[Virtual Network NAT](#): Virtual Network NAT (network address translation) simplifies outbound-only Internet connectivity for virtual networks. When configured on a subnet, all outbound connectivity uses specified static public IP addresses. Outbound connectivity is possible without a load balancer or public IP addresses directly attached to virtual machines.

[VPN Gateway](#): VPN Gateway lets customers establish secure, cross-premises connections between their virtual network within Azure and on-premises IT infrastructure. VPN gateway sends encrypted traffic between Azure virtual networks over the Microsoft network. The connectivity offered by VPN Gateway is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

[Virtual WAN](#): Virtual WAN is a networking service that brings many networking, security and routing functionalities together to provide a single operational interface. This service enables customers to automate large-scale branch connectivity which unifies network and policy management by optimizing routing using Microsoft global network.

Storage

[Azure Archive Storage](#): Azure Archive Storage offers low-cost, durable, and highly available secure cloud storage optimized to store rarely accessed data that is stored for at least 180 days with flexible latency requirements (of the order of hours).

[Azure Backup](#): Azure Backup protects Windows client data and shared files and folders on customer's corporate devices. Additionally, it protects Microsoft SharePoint, Exchange, SQL Server, Hyper-V virtual machines, and other applications in the customer's datacenter(s) integrated with System Center Data Protection Manager. Azure Backup enables customers to protect important data off-site with automated backup to Microsoft Azure. Customers can manage their cloud backups from the tools in Windows Server, Windows Server Essentials, or System Center Data Protection Manager. These tools allow the user to configure, monitor and recover backups to either a local disk or Azure Storage.

[Azure Data Box](#): Azure Data Box offers offline data transfer devices which are shipped between the customer's datacenter(s) and Azure, with little to no impact to the network. Azure Data Boxes use standard network-attached storage (NAS) protocols (Server Message Block (SMB)/CIFS and NFS), AES encryption to protect data, and perform a post-upload sanitization process to ensure that all data is wiped clean from the device. The data movement can be one-time, periodic, or an initial bulk data transfer followed by periodic transfers.

[Azure Data Lake Storage Gen1](#): Azure Data Lake Storage (Gen1) provides a single repository where customers can capture data of any size, type, and speed without forcing changes to their application as the data scales. In the store, data can be shared for collaboration with enterprise-grade security. It is also designed for high-performance processing and analytics from Hadoop Distributed File System (HDFS) applications (e.g., Azure HDInsight, Data Lake Analytics, Hortonworks, Cloudera, MapR) and tools, including support for low latency

workloads. For example, data can be ingested in real-time from sensors and devices for IoT solutions, or from online shopping websites into the store without the restriction of fixed limits on account or file size.

[Azure File Sync](#): Azure File Sync is used to centralize file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of any Azure file share.

[Azure HPC Cache](#): Azure HPC Cache is a file cache that speeds access to data for HPC tasks by caching files in Azure. It brings the scalability of cloud computing to existing workflows while allowing large datasets to remain in existing NAS or in Azure Blob storage.

[Azure Import/Export](#): Azure Import/Export allows customers to securely transfer large amounts of data to Azure Blob Storage by shipping hard disk drives to an Azure datacenter. Customers can also use this service to transfer data from Azure Blob Storage to hard disk drives and ship to their on-premises site. This service is suitable in situations where customers want to transfer several TBs of data to or from Azure, but uploading or downloading over the network is not feasible due to limited bandwidth or high network costs.

[Azure NetApp Files](#): Azure NetApp Files enables enterprise line-of-business and storage professionals to migrate and run complex, file-based applications with no code change. It is widely used as the underlying shared file-storage service in various scenarios. These include migration (lift and shift) of POSIX-compliant Linux and Windows applications, SAP HANA, databases, HPC infrastructure and apps, and enterprise web applications.

[Azure Site Recovery](#): Azure Site Recovery contributes to a customer's BCDR strategy by orchestrating replication of their servers running on-premises or on Azure. The on-premises physical servers and virtual machine servers can be replicated to Azure or to a secondary datacenter. The virtual machine servers running in any Azure region can also be replicated to a different Azure region. When a disaster occurs in the customer's primary location, customers can coordinate failover and recovery to the secondary location using Azure Site Recovery and ensure that applications / workloads continue to run in the secondary location. Customers can failback their workloads to the primary location when it resumes operations. It supports protection and recovery of heterogeneous workloads (including System Center managed / unmanaged Hyper-V workloads, VMware workloads). With Azure Site Recovery, customers can use a single dashboard to manage and monitor their deployment and also configure recovery plans with multiple machines to ensure that machines hosting tiered applications failover in the appropriate sequence.

[Azure Storage](#): Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. The Storage access control model allows each subscription to create one or more Storage accounts. Each Storage account has a primary and secondary secret key that is used to control access to the data within the Storage account. Every Storage service account has redundant data copies for fault tolerance. Listed below are the different storage types supported by Azure Storage:

- [Blobs](#) (including [Data Lake Storage Gen2](#)): Blobs is Microsoft's object storage solution for the cloud. Blobs can be used to store large amounts of binary data. For example, Blob Storage can be used for an application to store video, or to backup data. Azure Data Lake Storage Gen2 (a feature of Blobs) provides a hierarchical namespace, per object Access Control List (ACLs), and HDFS APIs.
- [Data Lake Storage Gen2](#): Data Lake Storage Gen2 is a highly scalable and cost-effective data lake solution for Big Data analytics. It combines the power of a high-performance file system with massive scale and economy to help accelerate time to insight. Data Lake Storage Gen2 extends Azure Blob Storage capabilities and is optimized for analytics workloads and compliant file system interfaces with no programming changes or data copying.
- [Disks](#): A managed or an unmanaged disk is a VHD that is attached to a VM to store application and system data. This allows for a highly durable and available solution while still being simple and scalable.
- [Files](#): Files offer shared storage for applications using the SMB protocol or Representational State Transfer (REST) protocol. Files can be used to completely replace or supplement traditional on-premises file servers or NAS devices. Applications running in Azure VMs, Cloud Services or from on-premises clients can access Files using SMB or REST.

- [Queues](#): Queues is a service for storing large number of messages. Queues provide storage and delivery of messages between one or more applications and roles.
- [Tables](#): Tables provide fast access to large amounts of structured data that do not require complex SQL queries. For example, Tables can be used to create a customer contact application that stores customer profile information and high volumes of user transaction.
- [Azure Disk Storage](#): Azure Disk Storage offers high throughput, high Input / Output Operations Per Second, and consistent low latency disk storage for Azure IaaS virtual machines. It allows the ability to dynamically change the performance of the SSD along with a customer's workloads without the need to restart VMs. Azure Disk Storage is suited for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads.
- [Cool Storage](#): Cool Storage is a low-cost storage tier for cooler data, where the data is not accessed often. Example use cases for Cool Storage include backups, media content, scientific data, compliance and archival data. Customers can use Cool Storage to retain data that is seldom accessed.
- [Premium Storage](#): Premium Storage delivers high-performance and low-latency storage support for virtual machines with input / output (IO) intensive workloads. Premium Storage is designed for mission-critical production applications.

[StorSimple](#): StorSimple is a hybrid cloud storage solution for primary storage, archiving, and disaster recovery. StorSimple optimizes total storage costs and data protection. It includes an on-premises Storage Area Network (SAN) solution that is a bottomless file server using Azure Blob Storage. StorSimple automatically arranges data in logical tiers based on current usage, age, and relationship to other data. Data that is most active is stored locally, while less active and inactive data is automatically migrated to the cloud. A StorSimple appliance is managed via the Azure Portal.

Databases

[Azure Arc-Enabled SQL Server](#): Azure Arc-Enabled SQL Server extends Azure services to SQL Server instances hosted outside of Azure, in the customer's data center, in edge site locations like retail stores, or any public cloud or hosting provider. Azure Arc enables customers to manage all of their SQL Servers from a single point of control. As customers connect their SQL Servers to Azure, they get a single place to view the detailed inventory of their SQL Servers and databases.

[Azure Cache for Redis](#): Azure Cache for Redis gives customers access to a secure, dedicated cache for their Azure applications. Based on the open source Redis server, the service allows quick access to frequently requested data. Azure Cache for Redis handles the management aspects of the cache instances, providing customers with replication of data, failover, and Secure Socket Layer (SSL) support for connecting to the cache.

[Azure Cosmos DB](#): Azure Cosmos DB was built from the ground up with global distribution and horizontal scale at its core. It offers turnkey global distribution across any number of Azure regions by transparently scaling and replicating customers' data wherever their users are. Customers can elastically scale throughput and storage worldwide, and pay only for the throughput and storage they need. Azure Cosmos DB guarantees single-digit-millisecond latencies at the 99th percentile anywhere in the world, offers multiple well-defined consistency models to fine-tune performance, and guarantees high availability with multi-homing capabilities - all backed by industry-leading, comprehensive SLAs.

[Azure Database for MariaDB](#): Azure Database for MariaDB is a relational database based on the open-source MariaDB Server engine. It is a fully managed database as a service offering that can handle mission-critical workloads with predictable performance and dynamic scalability.

[Azure Database for MySQL](#): Azure Database for MySQL is a relational database and a fully managed service built on Microsoft's scalable cloud infrastructure for application developers. Its built-in features maximize performance, availability, and security. Azure Database for MySQL empowers developers to focus on application innovation instead of database management tasks.

[Azure Database for PostgreSQL](#): Azure Database for PostgreSQL is a relational database and a fully managed service built on Microsoft's scalable cloud infrastructure for application developers. Its built-in features maximize performance, availability, and security. Azure Database for PostgreSQL empowers developers to focus on application innovation instead of database management tasks.

[Azure Database Migration Service](#): Azure Database Migration Service helps customers assess and migrate their databases and solve their compatibility and migration issues. The service is designed as a seamless, end-to-end solution for moving on-premises databases to the cloud.

[Azure Health Data Services](#): Azure Health Data Services is an API for clinical health data that enables customers to create new systems of engagement for analytics, machine learning, and actionable intelligence with health data. Azure Health Data Services improves health technologies' interoperability and makes it easier to manage data.

[Azure SQL](#): Azure SQL is a relational database service that lets customers rapidly create, extend, and scale relational applications into the cloud. Azure SQL delivers mission-critical capabilities including predictable performance, scalability with no downtime, business continuity, and data protection - all with near-zero administration. Customers can focus on rapid application development and accelerating time to market, rather than on managing VMs and infrastructure. Because the service is based on the SQL Server engine, Azure SQL provides a familiar programming model based on T-SQL and supports existing SQL Server tools, libraries and APIs.

[Azure Synapse Analytics](#): Azure Synapse Analytics, formerly known as SQL Data Warehouse, is a limitless analytics service that brings together enterprise data warehousing and Big Data analytics. It lets customers scale data, either on-premises or in the cloud. Azure Synapse Analytics lets customers use their existing T-SQL knowledge to integrate queries across structured and unstructured data. It integrates with Microsoft data platform tools, including Azure HDInsight, Machine Learning Studio, Azure Data Factory, and Microsoft Power BI for a complete data-warehousing and business-intelligence solution in the cloud.

[Microsoft Azure Managed Instance for Apache Cassandra](#): Microsoft Azure Managed Instance for Apache Cassandra provides automated deployment and scaling operations for managed open-source Apache Cassandra datacenters, accelerating hybrid scenarios and reducing ongoing maintenance.

[SQL Server Registry](#): SQL Server registry is a lightweight portal experience that enables customers to register their on-premises SQL Server instances to obtain Extended Security Updates (ESUs).

[SQL Server Stretch Database](#): SQL Server Stretch Database helps customers migrate warm and cold transactional data transparently and securely to Azure while still providing inexpensive long data retention times.

Developer Tools

[Azure App Configuration](#): Azure App Configuration allows customers to manage configuration within the cloud. Customers can create App Configuration stores to store key-value settings and consume stored settings from within applications, deployment pipelines, release processes, microservices, and other Azure resources. App Configuration allows customers to store and manage configurations effectively and reliably, in real time, without affecting customers by avoiding time-consuming redeployments.

[Azure DevTest Labs](#): Azure DevTest Labs helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost. Azure DevTest Labs creates labs consisting of pre-configured bases or Azure Resource Manager templates allowing customers to test the latest version of their application.

[Azure for Education](#): Azure for Education provides resources for students to learn about programming, cloud technologies, and world-class developer tools.

[Azure Lab Services](#): Azure Lab Services streamlines and simplifies setting up and managing resources and environments in the cloud. Azure Lab Services can quickly provision Windows and Linux virtual machines, Azure PaaS services, or complex environments in labs through reusable custom templates.

[Azure Load Testing](#): Azure Load Testing is a fully managed load-testing service that enables customers to generate high-scale load. The service simulates traffic for applications, regardless of where they are hosted. Developers, testers, and quality assurance (QA) engineers can use it to optimize application performance, scalability, or capacity.

[GitHub AE](#): GitHub AE is a security-enhanced and compliant way to use GitHub in the cloud. GitHub AE enables customers to move DevOps workload to the cloud while meeting stringent security and compliance requirements. GitHub AE is fully managed, reliable, and scalable, allowing the customer to accelerate delivery without sacrificing risk management. GitHub AE offers one developer platform from idea to production. Customers can increase development velocity, while maintaining industry and regulatory compliance with unique security and access controls, workflow automation, and policy enforcement.

Analytics

[Azure Analysis Services](#): Azure Analysis Services, based on the proven analytics engine in SQL Server Analysis Services, is an enterprise grade Online analytical processing engine and BI modeling platform, offered as a fully managed PaaS service. Azure Analysis Services enables developers and BI professionals to create BI semantic models that can power highly interactive and rich analytical experiences in BI tools and custom applications.

[Azure Data Explorer](#): Azure Data Explorer is a fast and highly scalable, fully managed data analytics service for real-time analysis on large volumes of data streaming from applications, websites, IoT devices and more. Azure Data Explorer makes it simple to ingest this data and enables customers to quickly perform complex ad hoc queries on the data.

[Azure Data Share](#): Azure Data Share is a simple and safe service for sharing data, in any format and any size, from multiple sources with other organizations. Customers can control what they share, who receives the data, and the terms of use via a user-friendly interface.

[Azure Stream Analytics](#): Azure Stream Analytics is an event-processing engine that helps customers gain insights from devices, sensors, cloud infrastructure, and existing data properties in real-time. Azure Stream Analytics is integrated out of the box with Event Hubs, and the combined solution can ingest millions of events and do analytics to help customers better understand patterns, power a dashboard, detect anomalies, or kick off an action while data is being streamed in real time. It can apply time-sensitive computations on real-time streams of data by providing a range of operators covering simple filters to complex correlations, and combining streams with historic records or reference data to derive business insights quickly.

[Data Catalog](#): Data Catalog is a fully managed service that serves as a system of registration and system of discovery for enterprise data sources. It lets users - from analysts to data scientists to developers - register, discover, understand, and consume data sources. Customers can use crowdsourced annotations and metadata to capture tribal knowledge within their organization, shine light on hidden data, and get more value from their enterprise data sources.

[Azure Data Factory](#): Azure Data Factory is a fully managed, serverless data integration service that refines raw data at cloud scale into actionable business insights. Customers can construct Extract, Transform, Load processes code free in an intuitive visual environment, and easily operationalize and manage the data pipelines at scale.

[Data Lake Analytics](#): Data Lake Analytics is a distributed analytics service built on Apache Yet Another Resource Negotiator that scales dynamically so customers can focus on their business goals and not on distributed infrastructure. Instead of deploying, configuring and tuning hardware, customers can write queries to transform data and extract valuable insights. The analytics service can handle jobs of any scale instantly by simply setting the dial for how much power is needed. Customers only pay for their job when it is running, making the service

cost-effective. The analytics service supports Azure Active Directory letting customers manage access and roles, integrated with on-premises identity system. It also includes U-SQL, a language that unifies the benefits of SQL with the expressive power of user code. U-SQL's scalable distributed runtime enables customers to efficiently analyze data in the store and across SQL Servers on Azure VMs, Azure SQL, and Azure Synapse Analytics.

Azure HDInsight: Azure HDInsight is a managed Apache Hadoop ecosystem offering in the cloud. It handles various amounts of data, scaling from terabytes to petabytes on demand, and can process unstructured or semi-structured data from web clickstreams, social media, server logs, devices, sensors, and more. Azure HDInsight includes Apache Hbase, a columnar NoSQL database that runs on top of the HDFS. This supports large transactional processing (Online Transaction Processing) of non-relational data, enabling use cases like interactive websites or having sensor data written to Azure Blob Storage. Azure HDInsight also includes Apache Storm, an open-source stream analytics platform that can process real-time events at large-scale. This allows processing of millions of events as they are generated, enabling use cases like IoT and gaining insights from connected devices or web-triggered events. Furthermore, Azure HDInsight includes Apache Spark, an open-source project in the Apache ecosystem that can run large-scale data analytics applications in memory. Lastly, Azure HDInsight incorporates R Server for Hadoop, a scale-out implementation of one of the most popular programming languages for statistical computing and machine learning. Azure HDInsight offers Linux clusters when deploying Big Data workloads into Azure.

Power BI Embedded: Power BI Embedded is a service which simplifies how customers use Power BI capabilities with embedded analytics. Power BI Embedded simplifies Power BI capabilities by helping customers quickly add visuals, reports, and dashboards to their apps, similar to the way apps built on Microsoft Azure use services like Machine Learning and IoT. Customers can make quick, informed decisions in context through easy-to-navigate data exploration in their apps.

AI + Machine Learning

AI Builder: AI Builder is integrated with Power Platform and Power Automate capabilities that help customers improve business performance by automating processes and predicting outcomes. AI Builder is a turnkey solution that brings the power of AI through a point-and-click experience. With AI Builder, customers can add intelligence to their applications with little to no coding or data science experience.

Azure Applied AI Services: Azure Applied AI Services is a portfolio of high-level services that enable developers to quickly unlock the value of data by applying AI into their key business scenarios. Built on top of the AI APIs of Azure AI Services, Azure Applied AI Services are optimized for critical tasks ranging from monitoring and diagnosing metric anomalies, mining knowledge from documents, enhancing the customer experience through transcription analysis, boosting literacy in the classroom, document understanding, etc.

Azure Bot Service: Azure Bot Service helps developers build bots / intelligent agents and connect them to the communication channels their users are in. Azure Bot Service solution provides a live service (connectivity switch), along with SDK documentation, solution templates, samples, and a directory of bots created by developers.

Azure Open Datasets: Azure Open Datasets service offers customers curated public datasets that can be used to add scenario-specific features to machine learning solutions for more accurate models. Azure Open Datasets are integrated into Azure Machine Learning and readily available to Azure Databricks and Machine Learning Studio (classic). Customers can also access the datasets through APIs and use them in other products, such as Power BI and Azure Data Factory. It includes public-domain data for weather, census, holidays, public safety, and location that helps customers train machine learning models and enrich predictive solutions.

Azure OpenAI Service: Azure OpenAI Service provides REST API access to OpenAI's language models including the GPT-3, Codex and Embeddings model series. These models can be adapted to the customer's specific task including content generation, summarization, semantic search, and natural language to code translation. Customers can access the service through REST APIs, Python SDK, or our web-based interface in the Azure OpenAI Studio.

[Azure Machine Learning](#): Azure Machine Learning (ML) is a cloud service that allows data scientists and developers to prepare data, train, and deploy machine learning models. It improves productivity and lowers costs through capabilities such as automated ML, autoscaling compute, hosted notebooks and ML Ops. It is open-source friendly and works with any Python framework, such as PyTorch, TensorFlow, or scikit-learn.

[Azure AI Services](#): Azure AI Services is the platform on which an evolving portfolio of REST APIs and SDKs enables developers to easily add intelligent services into their solutions to leverage the power of Microsoft's natural data understanding.

[Azure AI Services: AI Anomaly Detector](#): Azure AI Services: AI Anomaly Detector enables customers to monitor and detect abnormalities in time series data with machine learning. It utilizes an API which adapts by automatically identifying and applying the best-fitting models to data, regardless of industry, scenario, or data volume. Using time series data, the API determines boundaries for anomaly detection, expected values, and which data points are anomalies.

[Azure AI Services: Azure AI Vision](#): Azure AI Services: Azure AI Vision provides services to accurately identify and analyze content within images and videos. It also provides customers the ability to extract rich information from images to categorize and process visual data - and protect users from unwanted content.

[Azure AI Services: Azure AI Content Safety](#): Azure AI Services: Azure AI Content Safety is a suite of intelligent screening tools that enhance the safety of customer's platform. Image, text, and video moderation can be configured to support policy requirements by alerting customers to potential issues such as pornography, racism, profanity, violence, and more.

[Azure AI Services: Azure AI Custom Vision](#): Azure AI Services: Azure AI Custom Vision is an Azure AI Service that can train and deploy image classifiers and object detectors. The custom models trained by the AI service infer the contents of images based on visual characteristics.

[Azure AI Services: Face API](#): Azure AI Services: Face API is a service that has two main functions - face detection with attributes and face recognition. It provides customers the ability to detect human faces and compare similar ones, organize people into groups according to visual similarity, and identify previously tagged people in images.

[Azure AI Services: Azure AI Document Intelligence](#): Azure AI Services: Azure AI Document Intelligence is an Azure AI Service that uses machine learning technology to identify and extract text, key / value pairs and table data from form documents. It ingests text from forms and outputs structured data that includes the relationships in the original file. Customers receive accurate results that are tailored to specific content without heavy manual intervention or extensive data science expertise. Azure AI Document Intelligence is comprised of custom models, the prebuilt receipt model, and the layout API. Customers can call Azure AI Document Intelligence models by using a REST API to reduce complexity and integrate it into a workflow or an application.

[Azure AI Services: Azure AI Immersive Reader](#): Azure AI Services: Azure AI Immersive Reader is a service that lets customers embed text reading and comprehension capabilities into applications. Azure AI Immersive Reader helps users of any age and reading ability with features like reading aloud, translating languages, and focusing attention through highlighting and other design elements.

[Azure AI Services: Conversational Language Understanding](#): Azure AI Services: Conversational Language Understanding is a cloud-based API service that enables developers to build their custom language models (i.e., intent classifier and entity extractor). It enables its customers to integrate those custom machine-learning models into any conversational application, or unstructured text to predict, and pull out relevant, detailed information presented in a structured format i.e., JSON.

[Azure AI Services: Azure AI Metrics Advisor](#): Azure AI Services: Azure AI Metrics Advisor uses AI to perform data monitoring and anomaly detection in time series data. The service automates the process of applying models to the customer's data, and provides a set of APIs and a web-based workspace for data ingestion, anomaly detection, and diagnostics, without needing to know machine learning.

[Azure AI Services: Azure AI Personalizer](#): Azure AI Services: Azure AI Personalizer offers customers automatic model optimization based on reinforcement learning through a cloud-based API service that helps client applications choose the best, single content item to show each user. Personalizer collects and uses real-time information customers provide about content and context in order to select the most relevant content. Azure AI Personalizer uses system monitoring of customer and user behavior to report a reward score in order to improve its ability to select the best content based on the context information it receives. Content collected consists of any unit of information such as text, images, URLs, emails, and more.

[Azure AI Services: Question Answering](#): Azure AI Services: Question Answering is an Azure AI Services offering deployed on Azure. The endpoint is used by third party developers to create knowledge base endpoints. It allows users to distill information into an easy-to-navigate FAQ.

[Azure AI Services: Azure AI Speech](#): Azure AI Services: Azure AI Speech is an Azure service that offers speech to text, text to speech and speech translation using base (out of the box) and custom models.

[Azure AI Services: Text Analytics](#): Azure AI Services: Text Analytics is a cloud-based service that provides advanced natural language processing over raw text, and includes five main functions: sentiment analysis, key phrase extraction, named entities recognition, linked entities, and language detection.

[Azure AI Services: Translator](#): Azure AI Services: Translator is a cloud-based machine translation service, translating natural language text between more than 60 languages, via a REST-based web service API. Besides translation, the API provides functions for dictionary lookup, language detection and sentence breaking.

[Azure AI Services: Azure AI Video Indexer](#): Azure AI Services: Azure AI Video Indexer is a cloud application built as a cognitive video indexing platform that processes the videos that users upload and creates a cognitive index of the content within the video. It enables customers to extract the insights from videos using Video Indexer models.

[Machine Learning Studio \(Classic\)](#): Machine Learning Studio (Classic) is a service that enables users to experiment with their data, develop and train a model using training data and operationalize the trained model as a web service that can be called for predictive analytics.

[Autonomous Systems](#): Autonomous Systems enables automobile customers to develop, validate and deploy their autonomous driving capabilities. It provides an integrated solution that is extensible, highly automated and easy to use. It leverages key Azure services like storage, compute and various data platforms to enable a data driven development cycle.

[Microsoft Genomics](#): Microsoft Genomics offers a cloud implementation of the Burrows-Wheeler Aligner and the Genome Analysis Toolkit for secondary analysis which are then used for genome alignment and variant calling.

[Azure Health Bot](#): Azure Health Bot is an intelligent, highly personalized virtual health assistant that aims to improve the conversation between healthcare providers, payers and patients, via conversational navigation. It allows healthcare providers and payers to empower their users to get information related to their health, such as checking their symptoms, asking about their health plans, and receiving personalized, meaningful, credible answers, in an easy, self-serve and conversational way.

Internet of Things

[Azure Defender for IoT](#): Azure Defender for IoT provides customers with security protection by delivering unified visibility and control, adaptive threat prevention, and intelligent threat detection and response across IoT devices, IoT edges and IoT hubs running on-premises and in Azure cloud. It provides unified security management that enables end-to-end threat detection and analysis across hybrid cloud workloads and on customer's Azure IoT solution.

[Azure Digital Twins](#): Azure Digital Twins is an IoT platform that enables the customer's business to create a digital representation of real-world things, places, business processes, and people.

[Azure IoT Central](#): Azure IoT Central is a managed IoT SaaS solution that makes it easy to connect, monitor, and manage IoT assets at scale.

[Azure IoT Hub](#): Azure IoT Hub is used to connect, monitor, and control billions of IoT assets running on a broad set of operating systems and protocols. Azure IoT Hub establishes reliable, bi-directional communication with assets, even if they are intermittently connected, and analyzes and acts on incoming telemetry data. Customers can enhance the security of their IoT solutions by using per-device authentication to communicate with devices that have the appropriate credentials. Customers can also revoke access rights to specific devices to maintain the integrity of their system.

[Azure Sphere](#): Azure Sphere is a secured, high-level application platform with built-in communication and security features for Internet-connected devices. It comprises a secured, connected, crossover microcontroller unit, a custom high-level Linux-based OS, and a cloud-based security service that provides continuous, renewable security.

[Azure Time Series Insights](#): Azure Time Series Insights is used to collect, process, store, analyze, and query highly contextualized, time-series-optimized IoT-scale data. Time Series Insights is ideal for ad hoc data exploration and operational analysis. It is a uniquely extensible and customized service offering that meets the broad needs of industrial IoT deployments.

[Event Grid](#): Event Grid is a high scale Pub / Sub service which enables event-driven programming. It integrates with webhooks for delivering events.

[Event Hubs](#): Event Hubs is a Big Data streaming platform and event ingestion service capable of receiving and processing millions of events per second. Event Hubs can process, and store events, data, or telemetry produced by distributed software and devices. Data sent to an event hub can be transformed and stored by using any real-time analytics provider or batching / storage adapters. Event Hubs for Apache Kafka enables native Kafka clients, tools, and applications such as Mirror Maker, Apache Flink, and Akka Streams to work seamlessly with Event Hubs with only configuration changes. Event Hubs uses Advanced Message Queuing Protocol (AMQP), HTTP, and Kafka as its primary protocols.

[Microsoft Cloud for Sustainability](#): Microsoft Cloud for Sustainability enables customers to reach their environmental sustainability goals and advance their conservation efforts with secure, globally scalable, and innovative IoT solutions. Customers can reduce their energy usage in their factory or building, monitor the quality of their water output and decrease material waste spillage, and also to help prevent wildlife poaching and keep watch on endangered habitats.

[Notification Hubs](#): Notification Hubs is a massively scalable mobile push notification engine for sending notifications to Android, iOS, and Windows devices. It aggregates sending notifications through the Apple Push Notification service, Firebase Cloud Messaging service, Windows Push Notification Service, Microsoft Push Notification Service, and more. It allows customers to tailor notifications to specific customers or entire audiences with just a few lines of code and do it across any platform.

[Windows 10 IoT Core Services](#): Windows 10 IoT Core Services is a cloud subscription-based service that provides essential aids needed to commercialize a device on Windows 10 IoT Core. Through this subscription, Original Equipment Manufacturers (OEMs) have access to support channel, along with services to publish device updates and assess device health. Windows 10 IoT Core services offers monthly security and reliability updates, keeping devices stable and secure and utilizes Device Update Center to control device updates using the same content distribution network that is used by millions of customers to manage Windows updates.

Integration

[API Management](#): API Management lets customers publish APIs to developers, partners, and employees securely and at scale. API publishers can use the service to quickly create consistent and modern API gateways for existing backend services hosted anywhere.

[Azure Logic Apps](#): Azure Logic Apps automates the access and use of data across clouds without writing code. Customers can connect apps, data, and devices anywhere-on-premises or in the cloud, with Azure's large ecosystem of SaaS and cloud-based connectors that includes Salesforce, Office 365, Twitter, Dropbox, Google services, and more.

[Service Bus](#): Service Bus is a multi-tenant cloud messaging service that can be used to send information between applications and services. The asynchronous operations enable flexible, brokered messaging, along with structured first-in, first-out messaging, and publish / subscribe capabilities. Service Bus uses AMQP, Service Bus Messaging Protocol (SBMP), and HTTP as its primary protocols. Additionally, [Azure Relay](#) is a multi-tenant service offering that enables connectivity across network boundaries without normally required networking infrastructure.

Identity

[Azure Active Directory \(AAD\)](#): Azure Active Directory provides identity management and access control for cloud applications. To simplify user access to cloud applications, customers can synchronize on-premises identities, and enable single sign-on. AAD comes in three editions: Free, Basic, and Premium. Self-service credentials management is a feature of AAD that allows Azure AD tenant administrators to register for and subsequently reset their passwords without needing to contact Microsoft support. Microsoft Online Directory Services (MSODS) is also a feature of AAD that provides the backend to support authentication and provisioning for AAD.

[Azure Active Directory B2C](#): Azure Active Directory B2C extends Azure Active Directory capabilities to manage consumer identities. Azure Active Directory B2C is a comprehensive identity management solution for consumer-facing applications that can be integrated into any platform, and accessed from any device.

[Azure Active Directory Domain Services](#): Azure Active Directory Domain Services provides managed domain services such as domain join, group policy, LDAP, Kerberos / NTLM authentication that are fully compatible with Windows Server Active Directory (AD). Customers can consume these domain services without the need to deploy, manage, and patch domain controllers in the cloud. Azure Active Directory Domain Services integrates with the existing Azure Active Directory tenant, thus making it possible for users to log in using their corporate credentials.

[Azure Information Protection](#): Azure Information Protection controls and helps secure email, documents, and sensitive data that customers share outside their company walls. Azure Information Protection provides enhanced data protection capabilities to customers and assists them with classification of data using labels and permissions. Azure Information Protection includes Azure Rights Management, which used to be a standalone Azure service.

Management and Governance

[Application Change Analysis](#): Application Change Analysis is a subscription-level Azure resource provider. It checks for resource changes in the subscription, and provides data for various diagnostic tools to help users understand what changes might have caused issues.

[Automation](#): Automation lets customers create, deploy, monitor, and maintain resources in their Azure environment automatically by using a highly scalable and reliable workflow execution engine. Automation enables customers to create their PowerShell content (Runbooks) or choose from many available in the Runbook Gallery, and trigger job execution (scheduled or on-demand). Customers can also upload their own PowerShell modules and make use of them in their Runbooks. The distributed service takes care of executing the jobs per customer-specified schedule in a reliable manner, providing tenant context, tracking, and debugging as well as authoring experience.

[Azure Advisor](#): Azure Advisor is a personalized recommendation engine that helps customers follow Azure best practices. It analyzes Azure resource configuration and usage telemetry, and then provides recommendations that can reduce costs and improve the performance, security, and reliability of applications.

[Azure Blueprints](#): Azure Blueprints provides governed subscriptions to enterprise customers, simplifying largescale Azure deployments by packaging key environment artifacts, role-based access controls, and policies in a single blueprint definition.

[Azure Lighthouse](#): Azure Lighthouse offers service providers a single control plane to view and manage Azure across all their customers with higher automation, scale, and enhanced governance. With Azure Lighthouse, service providers can deliver managed services using comprehensive and robust management tooling built into the Azure platform. This offering can also benefit enterprise IT organizations by managing resources across multiple tenants.

[Azure Managed Applications](#): Azure Managed Applications enables customers to offer cloud solutions that are easy for consumers to deploy and operate. It can help customers implement the infrastructure and provide ongoing support. A managed application can be made available to all customers or only to users in the customer's organization by publishing it in the Azure marketplace or to an internal catalog, respectively.

[Azure Migrate](#): Azure Migrate enables customers to migrate to Azure, also serving as a single point to track migrations to Azure. Customers can choose from Microsoft first-party and Independent Software Vendor (ISV) partner solutions for their assessment and migration activities. Customers can plan and carry out migration of their servers using the Server Assessment and Server Migration tools; these are Microsoft solutions available on Azure Migrate. Server Assessment helps to discover on-premise applications and servers (Hyper-V and VMware VMs), and provides a migration assessment: a mapping from discovered servers to recommended Azure VMs, migration readiness analysis and cost estimates to run the VMs in Azure. It allows for dependency visualization to view dependencies of a single VM or a group of VMs. Server Migration allows customers to migrate the on-premises servers (non-virtualized physical or virtualized using Hyper-V and VMware) to Azure. Microsoft solutions to assess and migrate database workloads - Database Assessment and Database Migration - are also discoverable on Azure Migrate. In addition to these tools, ISV partner tools for assessment and migration are also discoverable on Azure Migrate. The machines discovered using these tools and the assessment and migration activities conducted using these tools can be tracked on Azure Migrate; this helps customers to track all their migration activities at one place.

[Azure Monitor](#): Azure Monitor provides full observability into a customer's applications, infrastructure and networks and collects, analyzes and acts on telemetry data from Azure and on-premises environments. It helps customers maximize performance and availability of applications and proactively identifies problems in real time. It includes, but is not limited to, the following four services: Azure Monitor Essentials, Application Insights, Application Insights Profiler, and Log Analytics.

- [Azure Monitor Essentials](#): Azure Monitor Essentials is a centralized dashboard which provides detailed up-to-date performance and utilization data, access to the activity log that tracks every API call, and diagnostic logs that help customers debug issues in their Azure resources.
- [Application Insights](#): Application Insights is used to monitor any connected App; It is on by default to be able to monitor multiple types of Azure resources, particularly Web Applications. It includes analytics tools to help diagnose issues and understand what users do with the App. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.
- [Application Insights Profiler](#): Application Insights Profiler is used to help understand and troubleshoot performance issues in production. It helps teams collect performance data in a low-impact way to minimize overhead to the system.
- [Log Analytics](#): Log Analytics enables customers to collect, correlate and visualize all their machine data, such as event logs, network logs, performance data, and more, from both on-premises and cloud assets. It enables transformation of machine data into near real-time operational intelligence for better decision making. Customers can search, correlate, or combine outputs of search from multiple data sources regardless of volume, format, or location. They can also visualize their data, separate signals from noise, with powerful log-management capabilities.

[Azure Policy](#): Azure Policy provides real-time enforcement and compliance assessment on Azure resources to apply standards and guardrails.

[Azure Resource Graph](#): Azure Resource Graph is a service designed to extend Azure Resource Management by providing efficient and performant resource exploration with the ability to query at scale across a given set of subscriptions so that customers can effectively govern their environment. Azure Resource Graph offers the ability to query resources with complex filtering, grouping and sorting by resource properties and the ability to iteratively explore resources based on governance requirements. Resource Graph also offers the ability to assess the impact of applying policies in a vast cloud environment.

[Azure Resource Manager \(ARM\)](#): Azure Resource Manager (ARM) enables customers to repeatedly deploy their app and have confidence that their resources are deployed in a consistent state. Customers can define the infrastructure and dependencies for their app in a single declarative template. This template is flexible enough for use across all customer environments such as test, staging, or production. If customers create a solution from the Azure Marketplace, the solution will automatically include a template that customers can use for their app. With Azure Resource Manager, customers can put resources with a common lifecycle into a resource group that can be deployed or deleted in a single action. Customers can see which resources are linked by any dependencies. Moreover, they can control who in their organization can perform actions on the resources. Customers manage permissions by defining roles and adding users or groups to the roles. For critical resources, they can apply an explicit lock that prevents users from deleting or modifying the resource. ARM logs all user actions so customers can audit those actions. For each action, the audit log contains information about the user, time, events, and status.

[Azure Signup Portal](#): Azure Signup Portal enables customers to sign up for Azure subscriptions. The service handles pre-requisites for signup such as Commerce account creation, Payment Instrument attachment, agreement acceptance, etc., and then finally funnels the user down to provisioning of a new subscription.

[Cloud Shell](#): Cloud Shell provides a web-based command line experience from Ibiza portal, Azure mobile, docs.microsoft.com, shell.azure.com, and Visual Studio Code. Both Bash and PowerShell experiences are available for customers to choose from.

[Cost Management](#): Cost management is an external offering for cloud cost management capabilities included with Azure subscriptions for financial governance for the customer's organization. It provides the ability to explore cost and usage data via multidimensional analysis, where creating customized filters and expressions allow the customer to answer consumption-related questions for their Azure resources.

[Microsoft Azure Portal](#): Microsoft Azure Portal provides a framework SDK, telemetry pipeline and infrastructure for Microsoft Azure services to be hosted inside the Azure Portal shell, and manages and monitors the required components to allow Azure services to run in a single, unified console. Azure is designed to abstract much of the infrastructure and complexity that typically underlies applications (i.e., servers, operating systems, and network) so that developers can focus on building and deploying applications. Microsoft Azure portal simplifies the development work for Azure service owners and developers by providing a comprehensive SDK with tools and controls for easily building and packaging the service applications. Customers manage these Azure applications through the Microsoft Azure Portal and Service Management API (SMAPI). Users who have access to Azure customer applications are authenticated based on their Microsoft Accounts (MSA) and / or Organizational Accounts. Azure customer billing is handled by MOCP. MOCP and MSA / Organizational Accounts and their associated authentication mechanisms are not in scope for this SOC report.

[Microsoft Purview](#): Microsoft Purview is a unified data governance service that helps customers manage and govern on-premises, multi-cloud, and SaaS data. Customers can easily create a holistic, up-to-date map of their data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.

[Azure Quotas](#): Azure Quotas enables Azure end customers to view and manage quotas for Azure Services by subscription. It provides the capability to request Quota increase inline for adjustable quotas and eliminate latency between the fulfillment and what customer can see in their portal.

Security

[Azure Confidential Computing](#): Azure Confidential Computing offers customers with solutions to enable isolation of sensitive data while it is being processed in the cloud. Azure Confidential Computing lets processing of data from multiple sources without exposing the input data to other parties. This type of secure computation enables many scenarios like anti-money laundering, fraud-detection, and secure analysis of healthcare data.

[Azure Dedicated HSM](#): Azure Dedicated HSM provides cryptographic key storage in Azure where the customer has full administrative control over the Hardware Security Module (HSM). It offers a solution for customers who require the most stringent security requirements.

[Azure Payment HSM](#): Azure Payment HSM is a bare metal Infrastructure as a Service (IaaS) that provides cryptographic key operations for real-time payment transactions in Azure. It is delivered using Thales payShield 10K payment HSMs and meets the most stringent payment card industry (PCI) requirements for security, compliance, low latency, and high performance.

[Microsoft Defender for Cloud](#): Microsoft Defender for Cloud helps customers prevent, detect, and respond to threats with increased visibility into and control over the security of Azure resources. It provides integrated security monitoring and policy management across Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions. Key capabilities include monitoring the security state of customer's Azure resources, policy-driven security maintenance, analysis of security data while applying advanced analytics, machine learning and behavioral analysis, prioritized security alerts as well as insights into the source of the attack and impacted resources.

[Microsoft Sentinel](#): Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise. Microsoft Sentinel aggregates data from all sources, including users, applications, servers, and devices running on-premises or in any cloud, letting customers reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of security solutions.

[Customer Lockbox for Microsoft Azure](#): Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data during a support request.

[Key Vault](#): Key Vault safeguards keys and other secrets in the cloud by using HSMs. It protects cryptographic keys and small secrets like passwords with keys stored in HSMs. For added assurance, customers can import or generate keys in HSMs that are FIPS 140-2 Level 2 certified. Key Vault is designed so that Microsoft does not see or extract customer keys. Customers can create new keys for Dev-Test in minutes and migrate seamlessly to production keys managed by security operations. Key Vault scales to meet the demands of cloud applications without the need to provision, deploy, and manage HSMs and key management software.

[Microsoft Azure Attestation](#): Microsoft Azure Attestation enables customers to verify the identity and security posture of a platform before the user interacts with it. Azure Attestation receives evidence from the platform, validates it with security standards, evaluates it against configurable policies, and produces an attestation token for claims-based applications. The service supports attestation of trusted platform modules (TPMs) and trusted execution environments (TEEs) and virtualization-based security (VBS) enclaves.

[Multi-Factor Authentication](#): Multi-Factor Authentication (MFA) helps prevent unauthorized access to on-premises and cloud applications by providing an additional layer of authentication. MFA follows organizational security and compliance standards while also addressing user demand for convenient access. MFA delivers strong authentication via a range of options, including mobile apps, phone calls, and text messages, allowing users to choose the method that works best for them.

Media

[Azure Media Services](#): Azure Media Services offers cloud-based versions of many existing technologies from the Microsoft Media Platform and Microsoft media partners, including ingest, encoding, format conversion, content protection and both on-demand and live streaming capabilities. Whether enhancing existing solutions or creating new workflows, customers can combine and manage Media Services to create custom workflows that fit every need.

Web

[Azure Cognitive Search](#): Azure Cognitive Search is a search as a service cloud solution that provides developers with APIs and tools for adding a rich search experience over customers' data in web, mobile, and enterprise applications.

[Azure Fluid Relay](#): Azure Fluid Relay is a managed offering for the Fluid Framework that helps developers build real-time collaborative experiences and replicate state across connected JavaScript clients in real-time. The Fluid Framework is a collection of client libraries for distributing and synchronizing shared state.

[Azure Maps](#): Azure Maps is a collection of geospatial services and SDKs that use fresh mapping data to provide geographic context to web and mobile applications. Azure Maps enables features such as map drawing, routing, search, time zones and traffic. The APIs can be subscribed to by customers in the Azure Portal or ARM.

[Azure SignalR Service](#): Azure SignalR service is a managed service to help customers easily build real-time applications with SignalR technology. This real-time functionality allows the service to push content updates to connected clients, such as a single page web or a mobile application. As a result, clients are updated without the need to poll the server or submit new HTTP requests for updates.

[Azure Spring Apps](#): Azure Spring Apps service makes it easy to deploy Spring Boot-based microservice applications to Azure with zero code changes. It manages the infrastructure of Spring Cloud applications, so developers can focus on their code. It provides lifecycle management using comprehensive monitoring and diagnostics, configuration management, service discovery, CI/CD integration, blue-green deployments, and more.

[Azure Web PubSub](#): The Azure Web PubSub service helps customers build real-time messaging web applications using WebSockets and the publish-subscribe pattern easily. This real-time functionality allows publishing content updates between server and connected clients (for example a single page web application or mobile application).

Mixed Reality

[Azure Remote Rendering](#): Azure Remote Rendering enables customers to render high quality interactive 3D content in the cloud and stream it in real-time to devices running on the edge.

[Azure Spatial Anchors](#): Azure Spatial Anchors helps customers create spatially aware mixed reality experiences across iOS, Android, and HoloLens devices. Customers can use this cross-platform service to unlock mixed reality capabilities like wayfinding, and enhance collaboration in facilities management, training, gaming, and other scenarios.

Internal Supporting Services⁶

Internal Supporting Services is a collection of services that are not directly available to third-party customers. They are included in SOC examination scope for Azure and Azure Government because they are critical to platform operations or support dependencies by first-party services, e.g., Office 365 and Dynamics 365.

Access Monitoring: Access Monitoring (AM) evaluates permissions throughout the infrastructure to report on effective access across Cloud + AI. AM drives reporting in the quarterly User Access Review and several KPIs inside the division.

AIP Masters: AIP Masters is a data processing pipeline that produces two business intelligence data sets (Azure Usage and Customer Catalog) used by other Azure services. The Azure Usage data set includes consumption data of Azure services by Azure customers at the subscription and meter level and the Customer Catalog dataset contains non-PII customer metadata and identifiers associated with Azure subscriptions.

Asimov Event Forwarder: Asimov Event Forwarder reads full event stream from OneDS Collector and breaks it apart into separate event streams based upon a set of subscription matching criteria. These event streams are then forwarded to the downstream services which subscribe to that stream.

Autopilot Security: Autopilot Security manages major parts of the security of the Azure core control plane, such as Certificate management and rollover, as well as the management of encryption and decryption keys. These services are related to Autopilot and Pilotfish systems that the rest of the Azure stack depends on.

AzCP Platform: AzCP Platform is a set of Service Fabric (SF) applications that install a SF cluster with a declarative deployment model paired with a collection of microservices to fill in gaps in the out-of-the-box support for common application needs within the Azure Control Plane.

Azure AI Services: Container Platform: Azure AI Services: Container Platform is the backend platform that hosts multiple Azure AI Services offerings.

Azure Marketplace Portal: Azure Marketplace Portal is the new marketplace for Azure applications. It is an online store for thousands of certified, open source, and community software applications, developer services, and data pre-configured for Azure.

Azure Code Scanning: Azure Code Scanning offers anti-malware scanning service for Azure service teams and services to protect against malware. Azure Code Scanning uses multiple anti-malware scanning engines to detect malware and Potentially Unwanted Programs (PUP).

Azure Diagnostic Services: Azure Diagnostic Services helps Azure customers and Support engineers to troubleshoot customer issues and identify root cause and recovery actions.

Azure Notebooks Component: Azure Notebooks Component is an internal service that allows Microsoft teams to embed a component that provides a Jupyter notebook canvas allowing teams to add themes, languages, etc. to their applications.

Azure Security Monitoring (ASM SLAM): ASM SLAM contains the features and services related to Security Monitoring in Azure. This includes Azure Security Pack which is deployed by services to configure their security monitoring.

Azure Service Health: Azure Service Health is a suite of experiences that provide personalized guidance and support when issues in Azure services are affecting or may affect customers in the future.

Azure Service Manager (RDFE): Azure Service Manager (RDFE) is a communication path from the user to the Fabric used to manage Azure services. It represents the publicly exposed classic APIs, which is the frontend to the Azure Portal and the SMAPI. All requests from the user go through Azure Service Manager (RDFE) or the newer ARM.

Azure Singularity: Azure Singularity is a managed High Performance Computing infrastructure service that provides highly reliable, low-cost infrastructure for AI training and inferencing. It provides lowest cost AI training and inferencing by driving high utilization via Secure, fine-grained multi-tenancy of 1P and 3P tenants; multiplexing of inferencing and training workloads; and Azure-wide, topology and workload-aware scheduling. It ensures high reliability through transparent and consistent checkpoint/restore, live migration, and elasticity, and global distribution of inferencing endpoints for single digit millisecond latencies and high availability. It supports integration for both 1P and 3P hardware; and pluggable data-planes and cluster schedulers.

Azure Stack Bridge: Azure Stack Bridge is an integration service which provides hybrid capabilities between

on-premise Azure Stack deployments and the online Azure cloud.

Azure Stack Edge Service: Azure Stack Edge Service, formerly known as Data Box Edge Service, manages appliances on customer premises that ingest data to customer storage account over network.

Azure System Lockdown: Azure System Lockdown is a feature within Azure Security Pack which monitors and audits applications running on other services in the execution environment.

Azure Watson: Azure Watson is an internal tool for service troubleshooting and crash dump analysis.

Blueshift Analytics: Blueshift Analytics is a Big Data service for internal Microsoft allowing them to run large scale batch jobs on data stored in Azure Data Lake Store (ADLS) gen 2.

Cloudfit: Cloudfit is a service that provides machine utilization analysis and recommendations to improve cost of goods sold (COGS) for all Microsoft services.

Copilot Applied AI: Copilot Applied AI (formerly Dynamics 365 Insights Apps AI and B360 AI Platform) provides internal AI services to products built by other teams within Dynamics 365 Insights Apps (formerly Business 360). The Dynamics 365 Insights Apps AI service leverages Microsoft data sources (Search Logs, Browser Logs) and other 1st and 3rd party data to enrich consumer profiles (B2C).

CoreWAN: CoreWAN is used to connect all Microsoft products worldwide to the Internet. It is composed of software, firmware, hardware devices, physical sites around the world, and terrestrial fiber optic cables, submarine fiber optic cables, and leased circuits from carriers.

CSCP-ReferenceSystems: CSCP Reference Systems enable the automation of capacity planning, management and execution with a set of data and services that are the “central source of truth” for Master Data with continuous validation of accuracy, freshness and completeness.

Datacenter Service Configuration Manager (dSCM): dSCM enables service teams to onboard to Azure Security internal services by providing specific configuration settings. The goal of dSCM is to reduce the onboarding and configuration management time for services onboarding to Azure Security services.

Datacenter Secrets Management Service (dSMS): dSMS is an Azure service that handles, stores, and manages the lifecycle for Azure Foundational Services.

Datacenter Security Token Service (dSTS): dSTS provides a highly available and scalable security token service for authenticating and authorizing clients (users and services) of Azure Foundation and Essential Services.

DataGrid: DataGrid system is comprised of a metadata repository system to store data contract for all Common Schema events and data ingested from SQL, Azure SQL, Azure Tables, Azure Queues, CSV and TSV files.

DesktopAnalytics⁵: DesktopAnalytics provides enterprise customers with device telemetry data to obtain and maintain accurate customer details across Office and Windows.

Dynamics 365 Integrator App: Dynamics 365 Integrator App is responsible for the sync of data between all Dynamics 365 platforms.

Enterprise Data Platform: Enterprise Data Platform is a data pipeline service that collects, analyzes and shares back value add telemetry to Microsoft Enterprise customers.

Environmental Sustainability Green SKU - Data Platform: Environmental Sustainability Green SKU - Data Platform provides science-based calculations for carbon emission computation for the Emission Impact Dashboard and Carbon platform.

Exp - Managed: Exp - Managed Service is an A/B testing platform which provides Microsoft teams with a tool to easily run A/B experiments.

Exp Treatment Assignment Service: Exp Treatment Assignment service provides HTTP REST endpoints for customers to retrieve configuration for A/B testing and exposure control. This includes variants (flights), feature flags (treatment variables), assignment context and the experimentation blob.

Fabric Controller Fundamental Services: Fabric Controller Fundamental Services, earlier known as Compute Manager, is an Azure core service responsible for the allocation of Azure tenants and their associated containers (VMs) to the hardware resources in the datacenter, and for the management of their lifecycle. Subcomponents include the Service Manager (SM / Aztec), Tenant Manager, Container Manager and Allocator.

Fabric Network Devices: Fabric Network Devices is used to provide all datacenter connectivity for Azure. Fabric Network Devices is completely transparent to Azure customers who cannot interact directly with any physical network device. The Fabric Network Devices service provides APIs to manage network devices in Azure datacenters. It is responsible for performing write operations to the network devices, including any operation that can change the code or configuration on the devices. The API exposed by Fabric Network Devices is used to perform certain operations, e.g., enable / disable a port for an unresponsive blade. It hosts all code and data necessary to manage network devices and does not have any dependency on services that are deployed after the build out.

Falcon⁵: Falcon is a pseudo-serverless ecosystem that enables teams across Microsoft to build highly scalable microservices powering various features that span across Bing, Skype and Office.

Gateway Manager: Gateway Manager is a control plane for VPN, ExpressRoute, Application Gateway, Azure Firewall, and Bastion. It is a critical component in Hybrid Azure Networking.

Geneva Analytics Orchestration: The Geneva Analytics Platform (Cloud Analytics Service) includes Data Studio, the Geneva Catalog, Geneva Job Scheduler, Geneva Collector and satellite micro-services. The Geneva Analytics Platform provides tools for Data Discovery, Data Transformations and Data Movement to internal Microsoft Teams. It integrates with other Azure Cloud Engineering Systems: The Geneva Pipeline, IcM, Geneva Health, etc.

Geneva Actions: Geneva Actions is an extensible platform enabling compliant management of production services and resources running on the Azure Cloud. It allows users to plug in their own live site operations to the Geneva Actions authorization and auditing system to ensure safe and secure control of the Azure platform.

Geneva Warm Path: Geneva Warm Path is a monitoring / diagnostic service used by teams across Microsoft to monitor the health of their service deployments.

Groups and Experimentation (OSG): Groups and Experimentation (OSG) Supports assignment of users and devices into groups for experimentation and targeting for scenarios such as OS build flighting, Storefront UX experiments, and DevCenter app Betas.

Holmes Service: Holmes service provides resource management and controls to trigger and influence actions on resources. Holmes is agnostic to specific types of service-model, & type of inventory, and tries to optimize packing, reshape clusters, apply required policies, and tools for various scenarios.

IcM Incident Management Service: IcM is a unified incident management system for all Microsoft services and provides tools for managing live site and on call rotations across the world.

Interflow: Interflow is a threat intelligence exchange service. It collects threat data (botnet IPs, hashes of malicious files, etc.) from various Microsoft teams and from various third parties, and then shares that data back out to Microsoft teams so they can act on it in their own products and services.

JIT: Just In Time (JIT) access provides engineers temporary elevated access to production services when needed to perform servicing activities and support their services.

Lens Explorer: Lens Explorer is part of the Geneva Analytics offering. It allows users to quickly drill down into customer's data and build dashboards that tell them a story.

CO+IE-Hardware Inventory: Cloud Operations and Innovation Engineering (CO+IE) Hardware Inventory provides users with information on metadata of physical assets in Cloud Operations and Innovation (CO+I) data centers.

MDM: MDM (Multi-Dimensional-Metrics) is the component within Geneva Monitoring responsible for collection and aggregation of metrics, performing alerting and visualizing health information.

MEE Privacy Service: MEE Privacy Service, also known as Next Generation Privacy Common Infrastructure, is a set of services that provides Data Subject Rights (DSR) distribution and auditing for internal Microsoft GDPR compliance. The service acts as the entry point for all view, export, delete and account close DSR signals that are then fanned out to various agents throughout the company to process in their data sets. Each of those agents then send back completion / acknowledgement signals that are subsequently used to produce several audit reports used to report Microsoft's GDPR compliance to executive management.

Microsoft Bot Framework: Microsoft Bot Framework represents the offline tools, SDKs, CLIs, etc. that support the Azure Bot Service offering.

Microsoft Emissions Impact Dashboard: The Emissions Impact Dashboard helps Microsoft cloud customers understand, track, report, analyze, and reduce carbon emissions associated with their cloud usage.

Microsoft Email Orchestrator: Microsoft Email Orchestrator (formerly called Azure Email Orchestrator) is an internal service for managing email content and for sending email communications to customers across Microsoft.

MSaaS File Management (DTM V2): MSaaS File Management is required to exchange files between customers, CSS, and Agents.

MSFT.RR DNS: MSFT.RR DNS is the Microsoft internal Recursive DNS for internal consumption.

Network Billing: Network Billing service provides a reliable pipeline with low-latency for services in Azure Networking.

On-Premises Data Gateway: On-Premises Data Gateway provides connectivity to on-premises resources for Power BI, Power Apps, and LogicApps services.

OneBranch Release: OneBranch Release is the release manager for services to deploy to all clouds in a secure and compliant manner.

OneDeploy Deployment Infrastructure (DE): OneDeploy Development Infrastructure is an Azure Deployment Engine (DE) custom workflow execution for Azure Foundational / Core services.

OneDS Collector: OneDS Collector is the ingestion front end for the telemetry pipelines used by Microsoft Windows, Microsoft Office and other Microsoft products. Microsoft products are instrumented with telemetry clients for logging and sending telemetry in the form of events. OneDS Collector validates and scrubs the events, then forwards them to the Asimov Event Forwarder service.

OneIdentity: OneIdentity is used for managing user accounts and security groups in different domains.

OneSettings: OneSettings service provides a command and control surface for numerous clients in the ecosystem. Primarily utilized to control the rate of Telemetry events collected by the Universal Telemetry Client (UTC) powering scenarios like Diagnostics, Experimentation and configuration.

PF-FC: PilotFish Fabric Controller (PF-FC) is the PilotFish hosted environment for managing the underlying hardware and services related to the Azure Fabric Controller. This includes buildout and management of the environments in PF, health of the nodes, FC role management and startup.

Pilotfish: Pilotfish is available to first-party customers (e.g., Office 365, Dynamics 365) for the management of hyper-scale services used in high-availability scenarios. Customers are guaranteed a defined level of service health, health monitoring, reporting and alerting, secure communications between servers, secure RDP capability, and full logical and physical machine lifecycle management.

SIPS ML Detections 2: SIPS ML Detections 2 service analyzes Azure logs to detect potential attacks compromises, such as account compromise, data breach, web attacks, compromised hosts, against Azure and Azure customers.

TuringAtAzure: TuringAtAzure is an API service that allows Microsoft product teams to access Turing language models in their production scenario.

Unified Remote Scanning (URSA): Unified Remote Scanning (URSA) provides a unified and standardized platform for remote security scans across Azure.

Vulnerability Scanning & Analytics: Vulnerability Scanning & Analytics is a service that provides vulnerability management and analytics for physical / virtual machines in cloud environments.

WaNetMon: WaNetMon monitors the health and availability of the Azure network and its services across all regions and all cloud environments. The platform provides monitoring, alerting and diagnostics capabilities for the Azure networking DRIs to quickly detect and diagnose issues. WaNetMon is also responsible for democratization of all network telemetry data, getting the data to a common data store and making it accessible for everyone.

Windows Azure Jumpbox: Windows Azure Jumpboxes are used by Azure service teams to operate Azure services. Jumpbox (hop-box) servers allow access to and from datacenters. They function as utility servers for runners, deployments, and debugging.

Workflow: Workflow lets users upload their workflows to Azure and have them executed in a highly scalable manner. This service is currently consumed only by O365 SharePoint Online service.

Microsoft Online Services

[Appsource:](#) Appsource is an enterprise app marketplace which integrates with other major Microsoft platforms including Dynamics and Office to allow an easy click-try-buy process.

[Dynamics 365 Customer Voice:](#) Dynamics 365 Customer Voice is a simple yet comprehensive survey solution that builds on the current survey-creation experience of Microsoft Forms in Microsoft 365. It offers new capabilities that make capturing and analyzing customer and employee feedback simpler than ever. Customers can respond to the surveys by using any web browser or mobile device. As responses are submitted, Power BI reports can be used to analyze them and make decisions in real time.

[Endpoint Attack Notifications:](#) Endpoint Attack Notifications is a managed threat hunting service that provides Security Operation Centers (SOCs) with expert level monitoring and analysis to help them ensure that critical threats in their unique environments do not get missed.

[Intelligent Recommendations:](#) Intelligent Recommendations enables businesses to automate relevant recommendations, including personalized results for new and returning users, and the ability to interpret both

user interactions and item or user metadata. In return, businesses receive tailored recommendations models based on their needs and business logic. Intelligent Recommendations frees companies from the tedious management of editorial collections. Instead, it helps drive engagement, run experiments, and build trust with consumers.

[Microsoft Defender for Cloud Apps](#): Microsoft Defender for Cloud Apps is a comprehensive service that provides customers the ability to extend their on-premise controls to their cloud applications and provide deeper visibility, comprehensive controls, and improved protection for these apps. Microsoft Defender for Cloud Apps provides Shadow IT discovery, information protection to cloud applications, threat detection and in-session controls.

[Microsoft Defender for Endpoint](#): Microsoft Defender for Endpoint is unified platform for preventative protection, post-breach detection, automated investigation, and response. Microsoft Defender for Endpoint protects endpoints from cyber threats, detects advanced attacks and data breaches, automates security incidents, and improves security posture.

[Microsoft Defender for Identity](#): Microsoft Defender for Identity is a cloud-based security solution that leverages on-premises Active Directory (AD) signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at the organization.

[Microsoft Graph](#): Microsoft Graph exposes multiple APIs from Office 365 and other Microsoft cloud services through a single endpoint. Microsoft Graph simplifies queries that would otherwise be more complex. Customers can use Microsoft Graph and Microsoft Graph Webhooks to:

- Access data from multiple Microsoft cloud services, including Azure Active Directory, Exchange Online as part of Office 365, SharePoint, OneDrive, OneNote, and Planner.
- Navigate between entities and relationships.
- Access intelligence and insights from the Microsoft cloud (for commercial users).

[Microsoft Intune](#): Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.

[Microsoft Managed Desktop](#): Microsoft Managed Desktop combines Microsoft 365 Enterprise with an IT-as-a-Service backed by Microsoft, for providing the best user experience, the latest technology as well as Desktop security and IT services, with an end-to-end cloud-based solution that is managed, supported, and monitored by Microsoft.

[Microsoft Stream](#): Microsoft Stream provides a common destination for video management, with built-in intelligence features, and the IT management and security capabilities that businesses of all sizes require. It is a fully managed SaaS service for enterprise customers in which users can upload, share and view videos within a small team, or across an entire organization, all inside a securely managed environment. Microsoft Stream leverages Azure AI services that enable in-video face detection and speech-to-text transcription that enhances learning and productivity. Microsoft Stream also includes IT admin capabilities for managing video content and increases engagement within an organization by integrating video into the applications used every day. Microsoft Stream utilizes built-in, industry-leading encryption and authenticated access to ensure videos are shared securely.

[Nomination Portal](#): Nomination Portal is an optimized customer relation management solution for Azure On-boarding and Nomination to Engagement Customer Lifecycle. It provides increased transparency on Azure services offered and what the customer is taking to production, a clearer idea of where IPs are needed with improved assignment and activity redecoration, as well as capturing effort towards customer engagements.

[PowerApps](#): PowerApps enables customers to connect to their existing systems and create new data, build apps without writing code, and publish and use the apps on the web and mobile devices. Services under PowerApps

include, but are not limited to, the following:

- **PowerApps Authoring Service:** PowerApps Authoring Service is a component service that supports the PowerApps service for authoring cross-platform applications without the need to write code. It provides the service to visually compose the app using a browser, to connect to data using different connections and APIs, and to generate a packaged application that is published to the PowerApps Service. The packaged application can be previewed using the service while authoring or it can be shared and played on iOS, Android and Windows Phone.
- **PowerApps MakerX Portal:** PowerApps MakerX Portal is the management website for PowerApps, where users can sign up for the product and perform management operations on PowerApps and related resources. It communicates directly with the PowerApps Service RP for most operations and provides entry points for users to launch into other PowerApps services as necessary.
- **PowerApps Service RP:** PowerApps Service RP is the back-end RESTful service for PowerApps that handles the management operations for PowerApps and related entities such as connections and APIs. Architecturally, the resource provider (RP) is an ARM RP, meaning that incoming requests are authenticated by the ARM on the front end and proxied through to the RP.

[Power Automate:](#) Power Automate helps customers set up automated workflows between their favorite apps and services to synchronize files, get notifications, collect data, and more.

[Power BI:](#) Power BI is a suite of business analytics tools to analyze data and share insights. Power BI dashboards provide a 360-degree view for business users with their most important metrics in one place, updated in real time, and available on all of their devices. With one click, users can explore the data behind their dashboard using intuitive tools that make finding answers easy. Power BI facilitates creation of dashboards with over 50 connections to popular business applications and comes with pre-built dashboards crafted by experts that help customers get up and running quickly. Customers can access their data and reports from anywhere with the Power BI Mobile apps, which update automatically with any changes to customers data.

[Power Virtual Agents:](#) Power Virtual Agents is an offering that enables anyone to create powerful chatbots using a guided, no-code graphical interface, without the need for data scientists or developers. It eliminates the gap between subject matter experts and the development teams building the chatbots, and the long latency between subject matter experts recognizing an issue and updating a chatbot to address it. It removes the complexity of exposing teams to the nuances of conversational AI and the need to write complex code. It also minimizes the IT effort required to deploy and maintain a custom conversational solution by empowering subject matter experts and departments to build and maintain their own conversational solutions.

[Windows Update for Business reports:](#) Windows Update for Business reports is a cloud-based solution that provides information about the customer's Azure Active Directory-joined devices' compliance with Windows updates. Windows Update for Business reports is offered through the Azure portal, and it's included as part of the Windows 10 or Windows 11 prerequisite licenses. Windows Update for Business reports helps customers monitor security, quality, driver, and feature updates for Windows 11 and Windows 10 devices, report on devices with update compliance issues, and analyze and display the customer's data in multiple ways.

Microsoft Dynamics 365

[Chat for Dynamics 365:](#) Chat for Dynamics 365 is one of the primary channels for customers to interact with support agents because of its simplicity and ease of use. Customer service centers prefer customers to connect via Chat for Dynamics 365 because it allows service agents to be more productive by simultaneously engaging with multiple customers.

[Dataverse:](#) Dataverse securely stores and manages data that is used by business applications. Data within Dataverse is stored within a set of entities (An entity is a set of records used to store data, similar to how a table stores data within a database). Dataverse includes a base set of standard entities that cover typical scenarios, but also lets the customer create custom entities specific to their organization and populate them with data using Power Query. App makers can then use Power Apps to build rich applications using this data.

[Dynamics 365 AI Customer Insights](#): Dynamics 365 AI Customer Insights is a cloud-based SaaS service that enables organizations of all sizes to bring together data from multiple sources and generate knowledge and insights to build a holistic 360 degree view of their customers.

[Dynamics 365 Athena - CDS to Azure Data Lake](#): Export to Data Lake (Athena) is a pipeline to continuously export data from the Dataverse to Azure Data Lake Gen2; it is designed for enterprise big data analytics, is cost-effective, scalable, has high availability / disaster recover capabilities and enables best in class analytics performance. Data is stored in the Common Data Model format which provides semantic consistency across apps and deployments. The standardized metadata and self-describing data in an Azure Data Lake Gen2 facilitates metadata discovery and interoperability between data producers and consumers such as Power BI, Azure Data Factory, Azure Databricks, and Azure Machine Learning service.

[Dynamics 365 Business Central](#): Dynamics 365 Business Central, formerly known as Dynamics NAV, is Microsoft's Small and Medium Business service built on and for the Azure cloud. It provides organizations with a service that supports their unique requirements and rapidly adjusts to constantly changing business environments, without the additional overhead of managing infrastructure.

[Dynamics 365 Business Q&A](#): Dynamics 365 Business Q&A (BizQA) services are enabled in Dynamics 365 Relevance Search (RS) by default. BizQA provides additional backend features to improve Dynamics 365 Relevance Search. These features include natural language search with Intent understanding, knowledge-based query annotation, semantic parsing to create structured queries, spell checking, query rewriting to normalize synonyms and abbreviations, and world common knowledge to understand location, date, time, holiday, and popular organizations. Additional features include multi-level ranking and a customer feedback loop which consumes user clicks to train and improve the rankers.

[Dynamics 365 Commerce \(including Dynamics 365 Retail\)](#), [Dynamics 365 Finance](#), and [Dynamics 365 Supply Chain Management](#): These offerings are supported by the same set of underlying services. These offerings provide customers with a complete set of adaptable ERP functionality that includes financials, demand planning, procurement / supply chain, manufacturing, distribution, services industries, public sector and retail capabilities that are combined with BI, infrastructure, compute and database services.

[Dynamics 365 Customer Insights Engagement Insights](#): Dynamics 365 Customer Insights Engagement insights enables customers to understand interactively how their customers are using their services and products - both individually and holistically - on websites, mobile apps, and connected products. Customers can combine behavioral analytics with transactional, demographic, survey, and other data types from Dynamics 365 Customer Insights.

[Dynamics 365 Customer Service](#): Dynamics 365 Customer Service provides tools / apps that help build great customer relationships by focusing on optimum customer satisfaction. It provides many features and tools that organizations can use to manage the services they provide to customers.

[Dynamics 365 Field Service](#): Dynamics 365 Field Service business application helps organizations deliver onsite service to customer locations. It combines workflow automation, algorithm scheduling, and mobility to help mobile workers fix issues when they are onsite at the customer location.

[Dynamics 365 Fraud Protection](#): Dynamics 365 Fraud Protection provides customers with a payment fraud solution helping e-commerce merchants drive down fraud loss, increase bank acceptance rates to yield higher revenue, and improve the online shopping experience for its customers.

[Dynamics 365 Guides](#): Dynamics 365 Guides is a mixed-reality application for Microsoft HoloLens that lets operators learn, during the flow of work by providing holographic instructions when and where they are needed. These instruction cards are visually tethered to the place where the work must be done, and can include images, videos, and 3D holographic models. Operators see what must be done, and where. Therefore, they can get the job done faster, with fewer errors and greater skill retention.

[Dynamics 365 Human Resources](#): Dynamics 365 Human Resources provides a Microsoft-hosted HR solution that delivers core HR functionality to HR professionals, managers and employees across the organization.

[Dynamics 365 Intelligent Order Management](#): Dynamics 365 Intelligent Order Management enables customers to manage the orchestration of orders through to fulfillment helping organizations orchestrate order flows across different platforms and apps. Intelligent Order Management is designed to operate in complex environments where there are many internal and external systems and partners that enable the supply chain processes. The platform is designed to scale up and down with a business, regardless of the organization size.

[Dynamics 365 Marketing](#): Dynamics 365 Marketing is a marketing-automation application that helps customers turn prospects into business relationships. Dynamics 365 Marketing has built-in intelligence to allow customers create emails and online content to support marketing initiatives, organize and publicize events, and share information.

[Dynamics 365 Project Operations](#): Dynamics 365 Project Operations connects sales, resourcing, project management, and finance teams in a single application to win more deals, accelerate project delivery, and maximize profitability.

[Dynamics 365 Remote Assist](#): Dynamics 365 Remote Assist enables customers to collaborate more efficiently by working together from different locations on HoloLens, HoloLens 2, Android, or iOS devices.

[Dynamics 365 Sales](#): Dynamics 365 Sales enables sales professionals to build strong relationships with their customers, take actions based on insights, and close sales faster. It can be used to keep track of customer accounts and contacts, nurture sales from lead to order, and create sales collateral.

[Dynamics 365 Sales Insights](#): Dynamics 365 Sales Insights empowers sellers to deliver personalized engagement and build profitable relationships. Capabilities include supercharging sales with a prioritized list of everything that needs to be done and optimizing the sales cadence for different types of prospects with sequences.

[Dynamics 365 Talent Attract & Onboard](#): Dynamics 365 Talent includes Attract, which can help customers identify, interview, and hire candidates that hold the skills the organization needs. As customers move from recruiting through hiring, the Onboard app can help customers bring the new employee into the organization by setting accurate expectations, providing information needed to get started, connecting them with colleagues, and set them up for success in their new role.

[Power Pages](#): Power Pages is where users can log-in and view an aggregated list of their business apps across various partner services including PowerApps.

Additionally, [Dynamics 365 Life Cycle Services](#) and [Power Platform Admin Center](#) are underlying features across multiple Dynamics 365 offerings. Dynamics 365 Life Cycle Services is a collaboration portal that provides an environment and a set of regularly updated services that can help customers manage the application lifecycle of their implementations of finance and operations apps. The Power Platform Admin Center provides a unified portal for administrators to manage environments and settings for Power Apps, Power Automate, and customer engagement apps.

Microsoft Cloud for Financial Services

[Microsoft Cloud for Financial Services](#): Microsoft Cloud for Financial Services provides capabilities to manage data to deliver differentiated experiences, empower employees, and combat financial crime. It also facilitates security, compliance, and interoperability. This set of cloud-based solutions enhances collaboration, automation, and insights to streamline processes; personalizes every customer interaction; improves customer experience; and delivers rich data insights. The data model enables Microsoft's partners and customers to extend the value of the platform with additional solutions to address the financial industry's most urgent challenges. These capabilities will help organizations align to business and operational needs, and then deploy quickly to accelerate time to value. Microsoft Cloud for Financial Services and its capabilities (Unified Customer Profile, Customer

Onboarding, and Collaboration Manager) are built atop Azure, Microsoft Dynamics 365, Microsoft Power Platform, and Microsoft 365 offerings. Microsoft 365 related offerings are not in the scope of this examination.

Unified Customer Profile: Unified Customer Profile helps banks tailor their customer experiences via a 360-degree view of the customer and, bringing together financial, behavioral, and demographic data.

Customer Onboarding: Customer Onboarding provides customers with easy access loan apps and self-service tools, helping to streamline the loan process to enhance customer experience and loyalty while increasing organizational and employee productivity. Helps customers efficiently apply for and keep track of a loan by streamlining the application process. Additionally, it empowers loan officers to manage loan applications with workflow automation, streamlining and customizing operations to meet specific lending needs.

Collaboration Manager: Collaboration Manager helps banks bring collaboration seamlessly into their lending workflows enabling them to improve process orchestration from front office to back office and facilitate omnichannel communications with customers. This capability helps banks improve organization and employee productivity, unlock value creation, and enhance customer experience. The portions of this capability covered by Microsoft 365 are not in scope for this examination.

Description of Controls

Security Organization	
Control Objective 1	Controls provide reasonable assurance that information security policies are defined, implemented and communicated.
Operator Access	
Control Objective 2	Controls provide reasonable assurance that logical access to production infrastructure is restricted to authorized personnel.
Operator Access	
Control Objective 3	Controls provide reasonable assurance that logical access to production platform and network infrastructure is restricted to authorized personnel.
Data Security	
Control Objective 4	Controls provide reasonable assurance that the data and secrets associated with the service are protected during transit and while at rest.
Change Management	
Control Objective 5	Control policies and procedures provide reasonable assurance that changes to the production platform are documented, authorized, and tested.
Software Development	
Control Objective 6	Controls provide reasonable assurance that development of new features or major changes to production platform follow a formal SDLC process and are documented, authorized and tested.
Vulnerability Management	
Control Objective 7	Controls provide reasonable assurance that the production platform is monitored for known security vulnerabilities and potential unauthorized activity.
Incident Management	
Control Objective 8	Controls provide reasonable assurance that production incidents are identified and responded to in accordance with documented procedures for timely resolution.
Physical and Environmental Security	
Control Objective 9	Control policies and procedures provide reasonable assurance that systems and data are protected against unauthorized physical access and environmental threats.
Logical Access	
Control Objective 10	Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.

Security Organization

Control Objective 1: Controls provide reasonable assurance that information security policies are defined, implemented and communicated.

Information Security Program

Azure has established an Information Security Program that provides documented management direction and support for implementing information security within the Azure environment. The design and implementation of applicable controls are defined based on the type of Azure service and its architecture.

The objective of the Information Security Program is to maintain the Confidentiality, Integrity, and Availability of information while complying with applicable legislative, regulatory, and contractual requirements.

The Information Security Program consists of the following components:

1. Policy, Standards and Procedures
2. Risk Assessment
3. Training and Awareness
4. Security Implementation
5. Review and Compliance
6. Management Reporting

The Information Security Program is based on the International Organization of Standards (ISO) Codes of Practice for information security management ISO / IEC 27001:2013 standard. Its accompanying policies and processes provide a framework to assess risks to the Azure environment, develop mitigating strategies and implement security controls. In addition, team specific Standard Operating Procedures (SOPs) are developed to provide implementation details for carrying out specific operational tasks in the following areas:

1. Access Control
2. Anti-Malware
3. Asset Management
4. Baseline Configuration
5. Business Continuity and Disaster Recovery
6. Capacity Management
7. Cryptographic Controls
8. Datacenter Operations
9. Document and Records Management
10. Exception Process
11. Hardware Change and Release Management
12. Incident Management
13. Legal and Regulatory Compliance
14. Logging and Monitoring
15. Network Security
16. Penetration Testing

17. Personnel Screening
18. Privacy
19. Risk Management
20. Security Development Lifecycle
21. Software Change and Release Management
22. Third Party Management
23. Training and Awareness
24. Vulnerability Scanning and Patch Management

Microsoft Security Policy

Microsoft Security Policy outlines the high-level objectives related to information security, defines risk management requirements and information security roles and responsibilities. The Security Policy contains rules and requirements that are met by Azure and other Online Services staff in the delivery and operations of the Online Services environment. The Security Policy is derived from the ISO / IEC 27001:2013 standard and is augmented to address relevant regulatory and industry requirements for the Online Services environment.

The policy is reviewed and updated, as necessary, at least annually, or more frequently, in case of a significant security event, or upon significant changes to the service or business model, legal requirements, organization or platform.

Each management-endorsed version of the Microsoft Security Policy and all subsequent updates are distributed to all relevant stakeholders from the Microsoft intranet site.

Roles and Responsibilities

Information security roles and responsibilities have been defined across the different Azure functions. The Cloud + AI Security team facilitates implementation of security controls and provides security guidance to the teams. The Global Ecosystem and Compliance team also coordinates with representatives from CELA (including leads of IT and Security), Human Resources (personnel security), and Microsoft Online Services (security policy requirements) on additional information security related activities impacting the services.

Personnel

Microsoft performs employee background screening as determined by the hiring manager based on access to sensitive data, including access to personally identifiable information or to back-end computing assets and per customer requirements, as applicable. Microsoft also employs a formal performance review process to ensure employees adequately meet the responsibilities of their position, including adherence to company policies, information security policies, and workplace rules. Hiring managers may, at their discretion, initiate corrective actions, up to and including immediate termination, if any aspect of an employee's performance and conduct is not satisfactory.

The Microsoft Online Services Delivery Platform Group works with Microsoft Human Resources and vendor companies to perform the required background check on each new or transferred personnel before they are granted access to the Microsoft Online Services production assets containing customer data.

Corporate policies are communicated to employees and relevant external parties during the onboarding process and as part of the annual security training and awareness education program. Non-disclosure Agreements (NDAs) are signed by employees and relevant external parties upon engagement with Microsoft. Disciplinary actions are defined for persons who violate the Microsoft Security Policy or commit a security breach. Employees are also required to comply with relevant laws, regulations and provisions regarding information security remain

valid if the area of responsibility changes or the employment relationship is terminated. Security Policy and non-disclosure requirements are reviewed periodically to validate appropriate protection of information.

Training and Awareness

Information security training and awareness is provided to Azure employees, contractors, datacenter personnel, and third parties on an ongoing basis to educate them on applicable policies, standards and information security practices. Awareness training on security, availability and confidentiality of information is provided to employees at the time of joining as part of induction. In addition, all staff participate in a mandatory security, compliance, and privacy training periodically in order to design, build and operate secure cloud services.

Employees receive information security training and awareness through different programs such as new employee orientation, computer-based training, and periodic communication (e.g., compliance program updates). These include training and awareness pertaining to the platform, in the security, availability, confidentiality, and integrity domains. In addition, job-specific training is provided to personnel, where appropriate. The key objectives of the information security training and awareness program are listed below:

Objective 1	The learner will be able to articulate the need to protect confidentiality, integrity, and availability of the production environment.
Objective 2	The learner will be able to apply basic security practices to safeguard the production environment and customer information.
Objective 3	The learner will understand the criticality of security, compliance and privacy in relation to customer expectations.
Objective 4	The learner will have a basic understanding of the responsibility to meet compliance and privacy commitments.
Objective 5	The learner will know where to find additional information on security, privacy, business continuity / disaster recovery and compliance.

All Engineering staff are required to complete a computer-based training module when they join the team. Staff are required to retake this training at least once per fiscal year.

In addition, annual SBC training is mandatory for all Microsoft employees. The SBC training includes an anti-corruption section that focuses on Microsoft’s anti-corruption policies and highlights policies that reinforce the need for employees to work with integrity and to comply with the anti-corruption laws of the countries in which Microsoft operates. All active employees are required to complete this course.

Operator Access

Control Objective 2: Controls provide reasonable assurance that logical access to production infrastructure is restricted to authorized personnel.

Production Infrastructure Access Management

Identity and Access Management (Microsoft Personnel)

The Security Policy establishes the access control requirements for requesting and provisioning user access for accounts and services. The policy requires that access be denied by default, follow least privilege principle, and be granted only upon business need.

Azure uses a specific corporate AD infrastructure for centralized authentication and authorization to restrict access to the systems and services within the Azure environment. Each user account is unique and is identifiable to an individual user.

Domain-account management requests are routed to the designated asset owner or associated agent according to established account provisioning and de-provisioning processes for approval. Typically, access is controlled through addition of individual user accounts to established domain security groups within the AD. Based on the configuration of a security group, any access request may either require explicit approval from the assigned security group owner or may be auto-approved for members of designated teams within Azure's organizational structure. Requests requiring explicit approval are automatically forwarded to the security group owner for approval in the system. In addition, Azure Government access requires explicit approval with required screening to confirm US citizenship of the user that is requesting access.

Employee status data from Microsoft HR is used to facilitate the provisioning and removal of user accounts in Azure-managed AD domains. Automated feeds from Microsoft HR systems provide this information, and account management processes prevent the creation of an account for individuals that do not have valid HR records. These feeds also initiate the removal of the user accounts for terminated users from the AD.

Automated mechanisms have been implemented to manage the appropriateness of access granted to information systems. Manual periodic reviews of individual accounts and security group memberships on assets are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation action is taken, as necessary, based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password expiration, length, complexity, and history. Multi-factor authentication is enforced for production domains that do not require password-based authentication. Azure personnel are required to follow the Microsoft password policy for applicable domains as well as local user accounts for all assets. Additionally, domain user accounts, if inactive for more than 90 days are suspended until the appropriateness of continued access for these accounts is resolved. If no action is taken by the user to reenable the suspended account, after 15 days the account is deleted.

Access to Azure Components

Access to the Azure components (e.g., Fabric, Storage, Subscriptions, and Network Devices) in the production environment is controlled through a designated set of access points and restricted to the corresponding service Production Support and Engineering teams. Access points such as Secure Admin Workstation (SAW) require users to perform two-factor authentication using a smart card and AD domain credentials to gain access. SAW is a secure hardened device which limits access to specific users and whitelisted applications.

Access to network devices in the scope boundary requires two-factor authentication. Passwords used to access Azure network devices are restricted to authorized individuals and system processes, based on job responsibilities and are changed on a periodic basis. Mobile devices connected to the production environment are limited to Secure Access Workstation (SAW) laptops and do not include phones or tablet.

In the unlikely event where JIT temporary access cannot be used, Azure service teams have the ability to access the production environment using designated break-glass accounts which provide user a short-term admin level access. Alerting and monitoring has been enabled for all break-glass accounts access. Upon accessing a break-glass account an alert is generated, whereupon the service team will investigate and determine if the access was appropriate.

Production assets that are not domain-joined or require local user accounts for authentication, require unique identifiers tied to individual user that requires appropriate approvals prior to being granted access. Non-domain-joined user accounts, that are not required due to termination of user or change in user's role and responsibilities, are removed manually within a stipulated period of termination / role change. In addition, access through persistent interactive local accounts on servers are not considered within user access review as they

are configured to raise security alert upon creations and are created on isolated VMs which tend to have a short life span.

Operator Access

Control Objective 3: Controls provide reasonable assurance that logical access to production platform and network infrastructure is restricted to authorized personnel.

Network Segregation

Packet Filtering

Azure has implemented filtering platform with rule sets and guards to ascertain that the untrusted VMs cannot generate spoofed traffic, cannot receive traffic not addressed to them, cannot direct traffic to protected infrastructure endpoints, and cannot send or receive inappropriate broadcast traffic.

VM based switch is designed and implemented through the filtering platform with Address Resolution Protocol (ARP) guards / rules to defend against ARP spoofing and related attacks. The guards / rules can be enabled on a per port basis to verify the sender's Media Access Control (MAC) Address and IP address to prevent spoofing of outgoing ARP packets, and only allow inbound ARP packets to reach a VM if they are targeted at that VM's IP address.

Storage nodes run only Azure-provided code and configuration, and access control is thus narrowly tailored to permit legitimate customer, applications, and administrative access only.

Virtual Local Area Network Isolation

Virtual Local Area Networks (VLANs) are used to isolate FC and other devices. VLANs partition a network such that no communication is possible between VLANs without passing through a router.

The Azure network in any datacenter is logically segregated into the Fabric core VLAN that contains trusted FCs and supporting systems and a VLAN that houses the rest of the components including the customer VMs.

In addition, supported virtualization standards for the Azure environment are available on the Microsoft public website.

Platform Secrets

Platform secrets, including certificates, keys, and Storage Account Keys (SAKs) are used for internal communication and are managed in a secure store that is restricted to authorized Azure personnel.

Access to Customer Virtual Machines by Azure Personnel

By default, user accounts are not created, and the Windows default administrator account is disabled on customer PaaS VMs. However, access to the customer VMs may be required for exceptional situations such as troubleshooting issues and handling incidents. In order to resolve these types of issues, temporary access procedures have been established to provide temporary access for Azure personnel to customer data and applications with the appropriate approvals. These temporary access events (i.e., request, approval and revocation of access) are logged and tracked using an internal ticketing system per documented procedures.

Network Device Remote Access

Azure network device access is provided through TACACS+ and local accounts, and follows standard logical access procedures as established by the Azure Networking team.

Directory and Organizational Identity Services Access Management

Customer Authentication Credentials

Each online customer is assigned a unique identity. Appropriate password hashing algorithms are in place to ensure that the authentication credential data stored is protected and is unique to a customer.

Remote Desktop

Production servers are configured to authenticate via AD. Directory and Organizational Identity Services' production servers require users to perform two-factor authentication using a smart card and domain password to gain access to the Microsoft Directory Store production servers using the Remote Desktop Connection application. Remote Desktop Connection has encryption settings enforced. These settings are controlled using the domain group policy within the production servers. The settings enforce remote desktop connections made to the production server to be encrypted.

Data Security

Control Objective 4: Controls provide reasonable assurance that the data and secrets associated with the service are protected during transit and while at rest.

Data Classification and Confidentiality Policy

Data (also referred to as information and asset) is classified into eleven categories, as described in the Data section above, based on how it is used or may be used within the Service environment.

There is one other type of data which is sometimes referenced in relation to data classification and protection. Azure does not treat this as a single category. Instead, it may contain data from one or more data classes described in the Data section above.

- **Personally Identifiable Information (PII):** Any data that can identify an individual is PII. Within Azure, PII of Azure subscription / tenant administrators (direct customers) is treated differently from the PII of end-users of services hosted in Azure. This is because in order to provide the Azure service, access to Administrator PII is needed, such as in the event of outage related notifications.

The General Data Protection Regulation (GDPR) introduces new rules for organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where they are located. The GDPR requires controllers to prepare a Data Protection Impact Assessment (DPIA) for operations that are 'likely to result in a high risk to the rights and freedoms of natural persons.' Microsoft performs an annual DPIA to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data.

Cryptographic Controls

Cryptographic controls and approved algorithms are used for information protection within the Azure platform and implemented based on the Azure Cryptographic Policy and Microsoft Cryptographic Standards. Cryptographic keys are managed throughout their lifecycle (e.g., ownership, generation, storage, distribution, periodic rotation, revocation, deactivation, and archival) in accordance with established key management procedures. Access to cryptographic keys is restricted through security groups membership and use of JIT. Azure provides customers the ability to manage their own data encryption keys.

Backup

Processes have been implemented for the backup of critical Azure components and data. Backups are managed by the Azure Data Protection Services (DPS) team and scheduled on a regular frequency established by the

respective component teams. The DPS team monitors backup processes for failures and resolves them per documented procedures to meet required backup frequency and retention. Azure teams that support the services and the backup process conducts integrity checks through standard restoration activities. Further, production data is encrypted on backup media.

Backup restorations are performed periodically by appropriate individuals. Results of the test are captured and any findings are tracked to resolution.

Offsite backups are tracked and managed to maintain accuracy of the inventory information. Azure is moving from offsite tape-based storage solutions to use of storage accounts in regions or locations different from the primary data location.

Access to backup data follows the same procedures defined under the Operator Access section above.

Data Protection Services

The DPS group has implemented a secure backup system infrastructure to provide secure backup, retention, and restoration of data in the Microsoft Online Services environment. Data is encrypted prior to backup and can be stored on tape, disk, or Storage accounts based on the service requirements.

Data Redundancy and Replication

Azure Storage provides data redundancy to minimize disruptions to the availability of customer data. The data redundancy is achieved through fragmentation of data into extents which are copied onto multiple nodes within a region. This approach minimizes the impact of isolated Storage node failures and loss of data.

Critical Azure components that support delivery of customer services have been designed to maintain high availability through redundancy and automatic failover to another instance with minimal disruption to customer services. Agents on each VM monitor the health of the VM. If the agent fails to respond, the FC reboots the VM. In case of hardware failure, the FC moves the role instance to a new hardware node and reprograms the network configuration for the service role instances to restore the service to full availability.

Customers can also leverage the geographically distributed nature of the Azure infrastructure by creating a second Storage account to provide hot-failover capability. In such a scenario, customers may create custom roles to replicate and synchronize data between Microsoft facilities. Customers may also write customized roles to extract data from Storage for offsite private backups.

Data is backed up to a region or location different from the primary data location and retained as per the retention policy.

Azure Storage maintains three replicas of customer data in blobs, tables, queues, files, and disks across three separate fault domains in the primary region. Customers can choose to enable geo-redundant storage, in which case three additional replicas of that same data will be kept also across separate fault domains in the paired region within the same geography. Examples of Azure Regions are North and South US or North and West Europe. These regions are separated by several hundred miles. Geo-replication provides additional data durability in case of a region wide disaster. For Azure Government, the geo-replication is limited to regions within the United States.

For Azure SQL that relies on Service Fabric, there are a minimum of three replicas of each database - one primary and two secondary replicas. If any component fails on the primary replica, Azure SQL detects the failure and fails over to the secondary replica. In case of a physical loss of the replica, Azure SQL creates a new replica automatically.

All critical platform metadata is backed up in an alternate region several hundred miles from the primary copy. Backup methods vary by service and include Azure Storage geo-replication, Azure SQL geo-replication, service-specific backup processes, and backup to tape. Azure manages and maintains all backup infrastructure.

Data Segregation

Directory Services assigns each tenant a unique identifier as part of the Active Directory. The mapping between the tenant and the AD location is represented within the partition table and is hidden from each customer tenant. Each tenant is segregated and partitioned within AD forest(s) based on this unique identifier to ensure appropriate customer data segregation.

Customer Data Deletion

Customer data is retained in the Online Service in a limited function account for 90 days after expiration or termination of customer's subscription so that the customer may extract the data. After the 90 day retention period ends, the customer's account is disabled and the customer's data is deleted. In accordance with applicable retention policies and legal / regulatory requirements as described in the Customer Registration section of the subscription, customer data is securely disposed of upon customer instruction. Hard disk and offsite backup tape destruction guidelines have been established for appropriate disposal. Customer accounts in non-payment or in violation of terms, etc., are subject to involuntary terminations and account disablement.

Platform Communication and Customer Secrets Protection

Data integrity is a key component of the Azure Platform. Customer secrets such as Storage Account Keys are encrypted during storage and transit. The customer facing portals and APIs only allow access to the Azure platform over a secure channel based on the service.

Azure Platform Communication

Internal communication between key Azure components where customer data is transmitted and involved is secured using SSL and TLS. SSL and TLS certificates are self-signed, except for those certificates that are used for connections from outside the Azure network (including the Storage service and the FC). These certificates are issued by a Microsoft Certificate Authority. Customer data is transmitted over a secure channel to the Azure platform services.

Customer Secrets

Customer secrets, including certificates, private keys, RDP passwords and SAKs are communicated through the SMAPI via the REST protocol, or Azure Portal over a secured channel using SSL. Customer secrets are stored in an encrypted form in Azure Storage accounts. Further, private root keys belonging to Azure services are protected from unauthorized access.

Access Control Service Namespace

Customers interact with the Access Control Service namespace over the web and service endpoints. Access Control Service namespace is only accessible through HTTPS and uses SSL to encrypt transmission of customer secrets including cryptographic keys, passwords and certificates over external networks. The customer information transmitted to all the Access Control Service endpoints is encrypted over external networks.

Change Management

Control Objective 5: Control policies and procedures provide reasonable assurance that changes to the production platform are documented, authorized, and tested.

The Change Management process has been established to plan, schedule, approve, apply, distribute, and track changes to the production environment through designated responsibilities with the objective of minimizing risk and customer impact. It further controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes.

Separation of Environments

Azure has implemented segregated environments for development, test and production, as a means to support segregation of duties and prevent unauthorized changes to production. Azure maintains logical and / or physical separation between the DEV (development), TEST (pre-production) and PROD (production) environments. Virtual services run on different clusters in separate network segments. TEST and PROD environments reside in separate network segments, which are accessed through distinct TEST and PROD Jumpboxes. Access to TEST and PROD Jumpboxes is restricted to authorized personnel from the service Operations and Production Support teams.

Deployment of software to production must meet testing and operational readiness criteria at each pre-production and production stage, and be approved prior to release. Production deployments use approved software builds and images.

In addition, production data is not used or copied to non-production environments. Test scripts and synthetic data are created for use in the development and test environments.

Segregation of Duties

Segregation of duties is established on critical functions within the Azure environment, to minimize the risk of unauthorized changes to production systems. Responsibilities for requesting, approving and implementing changes to the Azure environment are segregated among designated teams.

Software and Configuration Changes

Software and configuration changes within Azure, including major releases, minor releases, hot fixes, and emergency changes are managed through a formal change and release management procedure, and tracked using a centralized ticketing system. Changes are requested, approved, tracked and implemented throughout the release lifecycle, which includes product and engineering planning, release management, deployment and post-deployment support phases. Change requests are documented, assessed for their risks and evaluated / approved for acceptance by the designated Azure personnel. Software releases are discussed, planned, and approved through the daily coordinated meetings with appropriate representatives from the service and component teams.

Changes that are made to the source code are controlled through an internal source code repository. Refer to the Secure Development section for the controls enforced on the source code.

Formal security and quality assurance testing is performed prior to the software release through each pre-production environment (i.e., development and stage) based on defined acceptance criteria. The results of the quality assurance testing are reviewed and approved by the appropriate representatives prior to moving the release to production. For changes being deployed to the sovereign clouds, the change is tested in an Azure pre-production environment which is then deployed to the sovereign cloud production environment by the sovereign cloud data custodian after obtaining an additional approval from the sovereign cloud operator(s). Changes are reviewed for their adherence to established change and release management procedures prior to closure. Once deployed, changes are monitored for success; failed implementations are immediately rolled back and the change is not considered as completed until it is implemented and validated to operate as intended.

All activity performed, including changes made, using a user's break-glass account is logged and alerted. Service teams will review activity to ensure any changes made were appropriate.

Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.

Hardware Changes

Hardware changes are managed through formal change and release management procedures and a centralized ticketing system. Hardware changes are evaluated against the release entrance criteria that are established by the Azure Build-Out team, which forms the acceptance criteria for build-out of hardware within the Azure environment. Similar to software changes, the infrastructure changes are discussed and planned through the daily coordinated meetings with representatives from service and component teams.

The Azure Build-Out team coordinates scheduling of the release and deployment of the change into the production environment. The Azure Build-Out team performs the build-out of hardware devices and post build-out validation in coordination with the Azure Deployment Engineering team to verify its adherence to the hardware build requirements for new clusters. Azure Operations Managers perform final review and sign off of new deployments and Azure Build-Out team closes the ticket.

Network Changes

The Azure teams have implemented a formal change management process and centralized ticketing tool to document network changes and their approvals. Network changes include configuration changes, emergency changes, ACLs changes, patches, and new deployments.

ACL changes, that are identified and categorized as a standard change, are considered as pre-approved and may be implemented on peer review. Non-standard changes are reviewed for their characteristics and risks, and approved by representatives from the Cloud + AI Security and Networking teams, during the daily coordinated meeting. Reviews and approvals are also tracked in a centralized ticketing system. Changes are performed through approved change implementers that are part of a designated security group. Post-implementation reviews are performed by qualified individuals, other than the implementer, who evaluate the change success criteria.

Software Development

Control Objective 6: Controls provide reasonable assurance that development of new features or major changes to production platform follow a formal SDLC process and are documented, authorized and tested.

Secure Development

Azure's software development practices, across each of the component teams, are aligned with the Microsoft SDL methodology. The SDL introduces security and privacy control specifications during the feature / component design and throughout the development process, which are reviewed through designated security roles. Azure service teams track and complete their SDL compliance twice a year.

The Cloud + AI Security team creates the SDL baseline for Azure services to follow. The SDL baseline includes tasks to be performed which identify tools or processes that ensure teams are developing their services in a secured manner. As part of onboarding onto the SDL process, the Cloud + AI Security team works with the service teams to determine any additional SDL steps to be performed specific to the service. Additionally, teams are required to perform threat modeling exercises which are reviewed and approved by the Cloud + AI Security team. Each team has an SDL Owner who is responsible for ensuring appropriate completion of the SDL tasks. The SDL Owner reviews the SDL tasks and gives the overall sign off for completion of the SDL process.

Authorized system changes are promoted from test, pre-production and production per the software change and release management process as described in the Change Management section.

Source Code Control

The Azure source code is stored within Azure's internal source code repository tools that function as the versioning system for the source code. The tools track the identity of the person who checks source code out, and what changes are made. Permission to make changes to the source code is provided by granting write

access to the source code branches, which limits the access to confined project boundaries per job responsibilities. In addition, source code builds are scanned for malware prior to production release.

Access requests by full-time employees (FTEs) and non-FTEs to the source code repository require approval from the relevant project sponsor. Upon expiry, FTEs and non-FTEs need to submit access request to the project sponsor for renewal.

Vulnerability Management

Control Objective 7: Controls provide reasonable assurance that the production platform is monitored for known security vulnerabilities and potential unauthorized activity.

Logging and Monitoring

The Cloud + AI Security team has implemented agent-based monitoring infrastructure or custom script-based monitoring within the Azure environment to provide automated logging and alerting capabilities. The monitoring system detects potential unauthorized activity and security events such as the creation of unauthorized local users, local groups, drivers, services, or IP configurations. The monitoring agents are responsible for monitoring a defined set of user and administrator events, aggregating log events and sending the aggregated abnormal log information to a centralized log repository either at regular intervals or in real-time.

Component teams (e.g., Fabric and Storage) determine the specific events that need to be captured in consideration with a baseline. Administrator, operator, and system activities performed, such as logon / logoff within the Azure environment, are logged and monitored.

For network devices, the Azure Networking team monitors, logs, and reports on critical / suspicious activities and deviations from established baseline security configuration for the network devices. Predefined events are reported, tracked, and followed up on and security data is available for forensic investigations.

The Cloud + AI Security team has implemented an alerting system to provide real-time alerting through automatic generation of emails and alarms based on the log information captured by the monitoring infrastructure. Component teams are responsible for configuring the events to be alerted. The event and warning logs are routinely examined for anomalous behavior and when necessary, appropriate actions are taken in accordance with the incident handling procedures described in the Incident Management section. The Cyber Defense Operations Center (CDOC), Azure Live Site, and component teams manage response to malicious events, including escalation to and engaging specialized support groups.

Azure provides logging mechanisms that can be configured by customers to log activities and performance metrics related to their resources.

Microsoft operating system updates for virtual machines are made available through Microsoft Security Response Center (MSRC) site and Windows Update.

System Monitoring Tools

1. Geneva Monitoring within the Azure platform provides automated centralized logging and alerting capabilities for monitoring system use and detection of potential unauthorized activity. The Geneva Monitoring capabilities include Data Collection, Data Aggregation, Data Analysis and Information Access.
2. Alert and Incident Management System (IcM) provides alerting on a real-time basis by automatically generating emails and incident tickets based on the log information captured in Geneva Monitoring.
3. Azure Security Monitoring (ASM) provides logging and alerting capabilities upon detection of breaches or attempts to breach Azure platform trust boundaries. Critical security event logs generated are configured to alert through IcM. ASM monitors key security parameters to identify potentially malicious activity on Azure nodes.

4. Microsoft Endpoint Protection (MEP) guards against malware and helps improve security of the Azure PaaS Guest customers, Azure infrastructure tenants and Azure internal applications. MEP can be configured to enable antimalware protection for the Azure infrastructure tenants and Azure PaaS Guest VMs. Microsoft's antimalware endpoint solutions are designed to run quietly in the background without requiring human intervention. If malware is detected, the endpoint protection agent automatically takes action to remove the detected threat.
5. System Center Endpoint Protection (SCEP) guards against malware and helps improve security for Azure IaaS and physical servers. SCEP solution is designed to run in the background without requiring human intervention. If malware is detected, the endpoint protection agent automatically takes action to remove the detected threat.
6. ClamAV is implemented to monitor for malicious software in the Linux based server environment. If malware is detected, the endpoint protection agent automatically takes action to remove the detected threat.
7. Windows Defender guards against malware and helps improve security of the Azure PaaS, IaaS, and physical servers running Windows Server 2016 and newer. Windows Defender can be configured to enable antimalware protection for the Azure infrastructure tenants and Azure PaaS Guest VMs. Microsoft's antimalware solutions are designed to run quietly in the background without requiring human intervention. If malware is detected, the Windows Defender automatically takes action to remove the detected threat.

In addition, the Azure Live Site team uses third-party external monitoring services to monitor service health and performance.

Network Monitoring

The Networking team maintains a logging infrastructure and monitoring processes for network devices. In addition, the Azure Live Site team uses WaNetMon and third-party external monitoring services to monitor network connectivity. In addition, OneDDoS service is implemented on the Azure network to detect and respond to network-based attacks.

Vulnerability Scanning

Cloud + AI Security team carries out frequent internal and external scans to identify vulnerabilities and assess the effectiveness of the patch management process. Services are scanned for known vulnerabilities; new services are added to the next timed quarterly scan, based on their date of inclusion, and follow at least a quarterly scanning schedule thereafter. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed and identify vulnerabilities. The scanning reports are reviewed by appropriate personnel and remediation efforts are conducted in a timely manner.

Patching

The service and component teams are notified by the Microsoft Security Response Center (MSRC) upon identification of technical vulnerabilities applicable to the Azure Windows-based systems. Azure works with MSRC to evaluate patch releases and determine applicability and impact to Azure and other Microsoft Online Services environments and customers. For Linux based systems, the Ubuntu Security Notices for Linux patches are relied upon as the primary source. The applicable security patches are applied immediately or during a scheduled release to the Azure environment based on the severity of the vulnerability.

Processes are in place to evaluate patches and their applicability to the Azure environment. Once patches have been reviewed and their criticality level determined, service teams determine the release cadence for implementing patches without service disruption.

Applicable patches are automatically applied to Guest PaaS VMs unless the customer has configured the VM for manual upgrades. In this case, the customer is responsible for applying patches.

Teams follow a change process to modify the underlying OS within the platform. All changes are reviewed and tested, at a minimum, for their quality, performance, impact on other systems, recovery objectives and security features before they are moved into production using a defined release process. Test windows have been established for reviewing and testing of new features, and changes to existing features and patches.

Patches are released through the periodic OS release cycle in accordance with change and release management procedures. Emergency out-of-band security patches (e.g., Software Security Incident Response Process patches) are expedited for more immediate release.

Securing Edge Sites

All drives and operating systems used for production servers that reside in edge locations are encrypted. The drives have 'Always On' encryption and stay encrypted even during OS patching and updates. In addition, all unused IO ports on production servers that reside in edge locations are disabled by OS-level configurations that are defined in the baseline security configuration. Continuous configuration validation checks are enabled to detect drift in the OS-level configurations.

In addition, intrusion detection switches are enabled to detect physical access of the device. An alert is sent to an operator and the affected servers are shut down and its secrets are revoked. The alerting and tracking follows the incident response process as defined below.

Incident Management

Control Objective 8: Controls provide reasonable assurance that production incidents are identified and responded to in accordance with documented procedures for timely resolution.

Azure has implemented an incident management framework that includes defined processes, roles, communications, responsibilities and procedures for detection, escalation and response to incidents internally and to customers.

Security Incident - Internal Monitoring and Communication

Azure has established incident response procedures and centralized tracking tools which consist of different channels for reporting production system incidents and weaknesses. Automated mechanisms include system monitoring processes for alerting the Azure Live Site, CDOC, and service On-Call teams per defined and configured event, threshold or metric triggers. Incidents may also be reported via email by different Azure or Microsoft groups such as the service and component teams, Azure Support team or datacenter teams. The Azure Live Site, CDOC, and service On-Call teams provide 24x7 event / incident monitoring and response services. The teams assess the health of various components of Azure and datacenters, along with access to detailed information when issues are discovered. Processes are in place to enable temporary access to customer VMs. Access is only granted during, and for the duration of, a specific incident.

Additionally, CDOC conducts yearly tests of the Incident Management SOPs and response capabilities. Reports related to information security events are provided to Azure management on a quarterly basis. Problem statements for systemic issues are submitted to Information Security Management Forum for executive leadership review.

Incident Handling

Azure teams use the established incident classification, escalation and notification process for assessing an incident's criticality and severity, and accordingly escalating to the appropriate groups for timely action. The Azure Live Site and CDOC teams, with assistance from additional Azure teams (e.g., Cloud + AI Security team, component teams for investigation, when necessary), document, track, and coordinate response to incidents. Where required, security incidents are escalated to the privacy, legal or executive management team(s).

Incident Post-Mortem

Post-mortem activities are conducted for customer impacting incidents or incidents with high severity ratings (i.e., levels 0 and 1). The post-mortems are reviewed by the Azure Operations Management team during weekly and monthly review meetings with Azure senior management. Incident and security post-mortem trends are reviewed and evaluated on a periodic basis and, where necessary, the Azure platform or security program may be updated to incorporate improvements identified as a result of incidents.

Network Problem Management

The Networking team comprises Problem Management, Network Escalations, and Network Security teams to identify and address security alerts and incidents. The Networking team is responsible for identifying and analyzing potential problems and issues in the Microsoft Online Services networking environment.

Physical and Environmental Security

Control Objective 9: Control policies and procedures provide reasonable assurance that systems and data are protected against unauthorized physical access and environmental threats.

Datacenter Services

The Datacenter Management team has overall responsibility for the oversight of datacenter operations, including physical security, site services (server deployments and break-fix work), infrastructure build-out, critical environment operations and maintenance, and facilities management. Site Security Officers are responsible for monitoring the physical security of the facility 24x7x365.

Third-party vendors may perform various services in a Microsoft datacenter. For example:

- Mission critical vendors may be responsible for maintaining the datacenter's critical environment equipment.
- Security vendors may manage the site security guard force.
- General facilities management vendors may be responsible for minor building-related services, such as telephones, network, cleaning, trash removal, painting, doors, and locks.
- Site Services may support the Microsoft Online Services operations.

Datacenter Physical Security Management reviews and approves the incident response procedure on a yearly basis. The security incident response procedure details the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.

Physical Security

Main access to the datacenter facilities are typically restricted to a single point of entry that is manned by security personnel. The main interior or reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the Microsoft datacenters that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are restricted through various security mechanisms, such as electronic card access control, keyed lock on each individual door, man traps, and / or biometric devices.

Access Controls

The Datacenter Management team has implemented operational procedures to restrict physical access to only authorized employees, contractors, and visitors. Temporary or permanent access requests are tracked using a ticketing system. Badges are either issued or activated for personnel requiring access after verification of identification. The Datacenter Management team is responsible for reviewing datacenter access on a regular basis and for conducting a quarterly audit to verify individual access is still required.

Datacenter Security Personnel

Security personnel in the datacenter conduct the following activities for various datacenter facilities:

1. Man the security desks located at the main entrance of the datacenter
2. Conduct periodic inspections of the datacenter through walkthroughs
3. Respond to fire alarms and safety issues
4. Dispatch security personnel to assist service requests and emergencies
5. Provide Datacenter Management team with periodic updates about security events and entry logs
6. Operate and monitor datacenter surveillance systems

Security Surveillance

Datacenter surveillance systems monitor critical datacenter areas like datacenter main entry / exit, datacenter co-locations entry / exit, cages, locked cabinets, aisle ways, shipping and receiving areas, critical environments, perimeter doors, and parking areas. Surveillance recordings are retained for 90 days or as the local law dictates.

Emergency Power and Facility and Environmental Protection

Microsoft datacenter facilities have power backup and environmental protection systems. Datacenter Management team or the contracted vendor performs regular maintenance and testing of these systems.

Logical Access

Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.

Customer Data and Systems Access Management (Customers)

Customer Registration

Azure customers register for Azure services by setting up a subscription through the MOCP using a Microsoft Account or Organizational Account. Additionally, depending on the service, customers have the ability to register for the service via the service specific portal. MOCP, including billing and registration, and Microsoft Account / Organizational Account, including password management, are not in scope of this SOC report.

After registration, customers can request the creation of Storage accounts, hosted services, tenants, roles, and role instances within their subscription using the Azure Portal or programmatically through the SMAPI, which is the HTTPS interface exposed to external customers. The SMAPI allows customers to deploy and manage their services and their account. Among other things, this involves the ability to modify hosted services and Storage accounts, pick the geo-location for these accounts and place them in affinity groups, update configurations, 'swap' deployments and in essence, do all the non-creation related deployment / management operations that customers can do through the Azure Portal.

Additionally, customers can utilize the Azure Active Directory Graph API for programmatic access to Azure Active Directory through REST API endpoints. Applications can use the Graph API to perform create, read, update and delete (CRUD) operations on directory data and objects, e.g., common operations for a user object like create new users in directory, get user details, update user properties, and ascertain role-based access for user's group membership. Customers can also use the Azure Active Directory Module for Windows PowerShell cmdlets (provisioning API) to automate a number of deployment and management tasks. Azure has published a standard set of APIs with an ecosystem of tools and libraries on the Microsoft public website. All APIs or SDKs that services offer must be documented for interoperability and portability.

Virtual Machine Customization

Upon creation of a VM, the VM image includes customizations to performance, security and productivity. However, the image may be customized further by the customer to suit their needs. Hardening of the image is the responsibility of the customer. Access to the images may be restricted by the customer and updates to available images are communicated through customer-facing websites.

Identity and Access Management

Access to the Azure subscription through the Azure Portal is controlled by the Microsoft Account / Organizational Account. The ability to authenticate with the Microsoft Account / Organizational Account associated with the Azure subscription grants full control to all of the hosted services and Storage accounts within that subscription. (Note: Microsoft Account / Organizational Account and its associated authentication mechanisms are not in scope of this SOC report).

User sessions in the Azure portal can be configured by customers to automatically sign the user out of the Azure Portal session after a stipulated period of inactivity, protecting resources from unauthorized activity.

Location awareness technologies are implemented as part of the Azure Portal where location of the machine used for authentication is factored into the validation of the user identity. Where the user identity cannot be validated, Azure Portal would require the user to provide additional information to confirm their identity that could include MFA and / or secondary contact information for verification.

Applications can also access Azure services by using APIs (also known as SMAPI). SMAPI authentication is based on a user-generated public / private key pair and self-signed certificate registered through the Azure Portal. It is the customer's responsibility to safeguard the certificate.

The certificate is then used to authenticate subsequent access to SMAPI. SMAPI queues request to the Fabric, which then provisions, initializes, and manages the required application. Customers can monitor and manage their applications via the Azure Portal or programmatically through SMAPI using the same authentication mechanism.

In addition, customers can enable defined ports and protocols, e.g., RDP or SSH for Linux based services, on their instances and create local user accounts through the Azure Portal or SMAPI for debugging / troubleshooting issues with their applications. Customers are responsible for managing the local user accounts created.

Logic Apps allows users to run jobs such as calling HTTP/S endpoints or posting messages to Azure Storage queues on any schedule. Jobs can be integrated with user applications and can be configured to run immediately, or on a recurring schedule or anytime in the future. Jobs can be configured to call services both inside and outside of Azure. Jobs are processed as per the job settings defined by the customer. In case an error occurs during the processing, the job is retried based on the retry interval as mentioned by the customer. Errors are monitored and appropriate action is taken based on the settings defined by the customer. Jobs configured by customer administrators are executed within thirty (30) minutes of the scheduled job run and are repeated based on the defined recurrence settings.

Azure Automation allows users to create, monitor, manage, and deploy resources in the Azure environment using runbooks. These runbooks can be configured and schedules can be created to automate the manual, long-running, error-prone, and frequently repeated tasks that are commonly performed in a cloud environment.

Services initialize the resource groups within the Azure Portal based on the customer configured templates. A customer tenant can create an Azure Resource Manager using an ARM template. The template deploys and provisions all resources for any application in a single, coordinated operation. In the template, a customer tenant can define the resources that are needed for the application and specify deployment parameters to input values for different environments. The template consists of JSON and expressions which the customer tenant can use to construct values for their deployment.

Access to Customer Virtual Machines

External traffic to customer VMs is protected via ACLs but can be configured by the customer to allow external traffic only to customer designated ports and protocols. There is no port that is open by default unless explicitly configured by the customer in the service definition file. Once configured, the Azure Fabric Controller automatically updates the network traffic rule sets to allow external traffic only to the customer designated ports.

Customers can connect to their VMs via the ports and protocols defined by them, create credentials (i.e., username and password) and choose a certificate to encrypt the credentials during initial set-up. Authentication after set-up is performed using the self-created credentials. The connection is secured via Transport Layer Security (TLS) using a self-signed certificate generated by the VM instance. Customers can also upload custom certificates via the Azure Portal and configure their instances to use them securely.

Access to Customer Storage Account Data

Access to Azure Storage (i.e., blobs, tables, queues, files and disks) is governed by the SAK that is associated with each Storage account. Access to the SAK provides full control over the data in the Storage account.

Access to Azure Storage data can also be controlled through a Shared Access Signature (SAS). The SAS is created through a query template (URL), signed with the SAK. That signed URL can be given to another process, which can then fill in the details of the query and make the request of the Storage service. Authentication is still based on a signature created using the SAK, but it is sent to the Storage server by a third party. Access using the SAS can be limited in terms of validity time, permission set and what portions of the Storage account are accessible.

Data security beyond the access controls described above, such as fine-grain access controls or encryption, is the responsibility of the customer with exception to Managed Disk where encryption is enabled by default.

Identity and Access Management - Self Service Password Reset

Self-Service Password Reset (SSPR) for users is a feature which allows end-users in customer organization to reset their passwords automatically without calling an administrator or helpdesk for support. SSPR has three main components:

1. **Password Reset Policy Configuration Portal** - Administrators can control different facets of password reset policy in the Azure Portal.
2. **User Registration Portal** - Users can self-register for password reset through a web portal.
3. **User Password Reset Portal** - Users can reset their own passwords using a number of different challenges in accordance with the administrator-controlled password-reset policy.

Customer Administrative Passwords

The One Time Password (OTP) generation module is implemented as a worker role within the Azure AD platform and OTP used for self-service password reset are randomly generated. These OTPs expire after their usage or a pre-defined time limit. OTP generated for email and SMS are validated. Additionally, the OTP values are to be provided within the same session where the OTP was requested.

For the password reset process, the only information displayed within the HTTPS response packets is the masked phone number and cookies required to reset the password. The new passwords supplied by customer administrators within the SSPR portal adhere to the Azure AD password policy requirements. The SSPR portal is only accessible through HTTPS port and the new passwords supplied by the customers are encrypted during transmission over external networks.

This also applies to the initial temporary password generated for the user. These temporary passwords have a pre-defined time limit before it expires and forces users to change it on first usage.

Quotas and Thresholds

Where applicable, quotas are enforced on Azure services as configured by the service administrators. Quota name, the threshold value for the quota, and the behavior on exceeding the quota, have been specified to protect customer entities from availability related issues.

Complementary User Entity Controls

The following list includes complementary user entity controls that Azure assumes its user entities have implemented. User entities' auditors should determine whether the user entities have established sufficient controls in these areas:

Complementary User Entity Controls	Related Control Objectives
Customers are responsible for establishing appropriate controls over the use of their Microsoft Accounts and passwords.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for disabling / deleting account access to their Azure services upon employee and contractor role change or terminations.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers' administrators are responsible for the selection and use of their passwords.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for protecting the credentials associated with their deployment profiles.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for specifying strong credentials used with service identities and management service accounts and managing them for continued appropriateness.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for ensuring the confidentiality of any user IDs and passwords used to access MFA systems.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible to assign unique IDs and secured passwords to users and customers accessing their instance of the API Management service.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.

Complementary User Entity Controls	Related Control Objectives
Customers are responsible for ensuring that user IDs and passwords are assigned to authorized individuals.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for selection of the access mechanism (i.e., public or signed access) for their data.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for appropriate protection of the secrets associated with their accounts.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for securing certificates used to access Azure SMAPI.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for securing certificates used to access Intune (iOS Onboarding certificate, Windows Phone Code Signing Certificates for Windows Phone, any certificate used to sign Enterprise Windows Applications, and Certificate Registration Point (CRP) Signing certificates used in VPN / WiFi Profiles).	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for implementing appropriate authentication mechanisms and only granting admin access to appropriate individuals to maintain the integrity of their AAD tenant.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers utilizing AAD services are responsible for implementing appropriate authentication mechanisms and limiting admin access to appropriate individuals to maintain integrity of their SaaS applications.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible to implement logical access controls to provide reasonable assurance that unauthorized access to key systems will be restricted.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for ensuring the supervision, management and control for access to key systems hosted in the Azure environment.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for reporting to Microsoft the incidents and alerts that are specific to their systems and Azure.	Control Objective 8: Controls provide reasonable assurance that production incidents are identified and responded to in accordance with documented procedures for timely resolution.

Complementary User Entity Controls	Related Control Objectives
Customers are responsible for immediately notifying the MFA service of any actual or suspected information security breaches, including compromised user accounts.	Control Objective 8: Controls provide reasonable assurance that production incidents are identified and responded to in accordance with documented procedures for timely resolution.
Customers are responsible for appropriately testing application systems deployed in the Dynamics 365 environment prior to deployment in the production environment.	Control Objective 5: Control policies and procedures provide reasonable assurance that changes to the production platform are documented, authorized, and tested.
Customers are responsible for appropriately testing and approving customer developed customizations and extensions prior to deployment in the Dynamics 365 production environment.	Control Objective 5: Control policies and procedures provide reasonable assurance that changes to the production platform are documented, authorized, and tested.
Customers are responsible for validating the completeness and accuracy of customized reporting in the Dynamics 365 environment.	Control Objective 5: Control policies and procedures provide reasonable assurance that changes to the production platform are documented, authorized, and tested.
Customers are responsible for the authorization of transactions processed in the Dynamics 365 system.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for notifying Microsoft of any unauthorized use of Dynamics 365 accounts.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for hardening virtual machine images as per their requirements.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.
Customers are responsible for responding to data subject requests for customer data or system generated logs.	Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.

Changes to the Azure system

The only changes to the Azure system from July 1, 2022 to June 30, 2023 that would affect report users' understanding of how the system is used were changes in offerings/services, datacenter locations, and edge sites. Refer to the updated list of offerings/services, datacenter locations, and edge sites in the "Azure and Azure Government Report Scope and Boundary" and "Regions covered by this Report" subsections in Section III of this SOC 1 report.

System Incidents

There were no significant system incidents identified that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the control objectives or (b) otherwise resulted in a significant failure in the achievement of one or more of those control objectives during the period July 1, 2022 to June 30, 2023.

Section IV: Information Provided by Independent Service Auditor Except for Control Objectives and Control Activities

Section IV: Information Provided by Independent Service Auditor Except for Control Objectives and Control Activities

Introduction

This report on the description of the system is intended to provide user entities and their auditors with information for their evaluation of the effect of a service organization on a user entity's internal control relating to Microsoft Corporation's (Microsoft) controls over its in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenter ("Azure") for the Azure and Azure Government cloud environments, during some or all of the period July 1, 2022 through June 30, 2023.

This section presents the following information provided by Microsoft:

- The control objectives specified by the management of Microsoft.
- The controls established and specified by Microsoft to achieve the specified control objectives.

Also included in this section is the following information provided by Deloitte & Touche LLP:

- A description of the tests performed by Deloitte & Touche LLP to determine whether Microsoft's controls were operating with sufficient effectiveness to achieve specified control objectives. Deloitte & Touche LLP determined the nature, timing, and extent of the testing performed.
- The results of Deloitte & Touche LLP's tests of controls.

Our examination was conducted in accordance with the American Institute of Certified Public Accountants' (AICPA) Attestation Standards and International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organization, issued by the International Auditing and Assurance Standards Board, and standard 951 established by the Institut der Wirtschaftsprüfer. AICPA Attestation Standards are inclusive of the following: (1) AT-C 105, *Concepts Common to all Attestation Engagements*; (2) AT-C 205, *Examination Engagements*; and (3) AT-C 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*. Our testing of Microsoft's controls was restricted to the control objectives and related control activities listed in this Section IV and was not extended to controls described in Section III but not included in Section IV, or to controls that may be in effect at user organizations.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities obtain an understanding and to assess control risk at the user entities. The controls at user entities, and Microsoft's controls should be evaluated together. If effective user entity controls are not in place, Microsoft's controls may not compensate for such weaknesses.

Control environment elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Microsoft, our procedures included tests of the following relevant elements of Microsoft's control environment:

1. Integrity and Ethical Values
2. Microsoft Standards of Business Conduct
3. Training and Accountability
4. Commitment to Competence

- 5. Compliance & Ethics, Internal Audit, Audit Committee
- 6. Risk Assessment
- 7. Monitoring
- 8. Information and Communication

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Microsoft’s activities and operations, inspection of Microsoft’s documents and records, and reperformance of the application of Microsoft’s controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

Controls within the control environment have been categorized into the following domains:

- 1. Information Security (IS)
- 2. Operator Access (OA)
- 3. Data Security (DS)
- 4. Change Management (CM)
- 5. Security Development Lifecycle (SDL)
- 6. Vulnerability Management (VM)
- 7. Incident Management (IM)
- 8. Physical and Environmental Security (PE)
- 9. Logical Access (LA)
- 10. Additional Edge Sites Logical Access Controls (ED)

Tests of operating effectiveness

Our tests of the controls were designed to cover a representative number of transactions throughout the period from July 1, 2022 through June 30, 2023. In determining the nature, timing and extent of tests, we considered, (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the nature of the control objectives to be met, (d) the assessed level of control risk, (e) the expected effectiveness of the test, and (f) the results of our tests of the control environment.

Description of testing procedures performed

Deloitte & Touche LLP performed a variety of tests relating to the controls listed in this section throughout the period from July 1, 2022 through June 30, 2023. Our tests of controls were performed on controls as they existed during the period July 1, 2022 through June 30, 2023 and were applied to those controls relating to control objectives specified by Microsoft.

In addition to the tests listed below, ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period. Tests performed are described below:

Test	Description
Corroborative Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.

Test	Description
Observation	Observed the performance of the control during the report period to evidence application of the specific control activity.
Examination of documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperfomed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Reperformance of programmed processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Reliability of information produced by the Service Organization

We performed procedures to evaluate whether the information provided by Microsoft, which includes (a) information provided by Microsoft to the service auditor in response to ad hoc requests from the service auditor (e.g., population lists); (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations); and (c) information prepared for user entities (e.g., user access lists), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes. Information we utilized as evidence may have included, but was not limited to:

- Standard “out of the box” reports as configured within the system
- Parameter-driven reports generated by Microsoft’s systems
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
- Spreadsheets that include relevant information utilized for the performance or testing of a control
- Analysis, schedules, or other evidence manually prepared and utilized by Microsoft

Our procedures to evaluate whether this information was sufficiently reliable included obtaining evidence regarding the accuracy and completeness included procedures to address (a) the accuracy and completeness of source data and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by Microsoft.

Reporting on results of testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because Deloitte & Touche LLP does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all deviations.

Results of Testing Performed

Security Organization

Control Objective 1: Controls provide reasonable assurance that information security policies are defined, implemented and communicated.

Control ID	Control Activity	Test Procedures	Results of Tests
IS - 1	A security policy that defines the information security rules and requirements for the Service environment has been established and communicated.	<ul style="list-style-type: none">• Inquired of management if a documented security policy that specifies the documented rules and requirements applicable to the Microsoft Azure environment exists.• Obtained and inspected Microsoft Azure's Information Security Policy and ascertained that it addressed applicable information security requirements.• Observed that the Security Policy document was published and communicated to Microsoft Azure employees and the relevant third parties.• Inspected the Security Policy to determine if the security objectives were derived from the corporate objectives and business processes, relevant laws and regulations as well as the current and future expected threat environment with respect to information security.	No exceptions noted.
IS - 2	The Security Policy is reviewed and approved annually by appropriate management.	<ul style="list-style-type: none">• Inquired of management to gain an understanding of the process for reviewing and approving the Microsoft Azure security policy.• Obtained and inspected the latest policy review performed for the Microsoft Azure security policy and approval provided by management.	No exceptions noted.
IS - 3	Management has established defined roles and responsibilities	<ul style="list-style-type: none">• Inquired of management to gain an understanding of the implementation of security policy requirements	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	to oversee implementation of the Security Policy across Azure.	<p>within Microsoft Azure through the designation of roles and responsibilities.</p> <ul style="list-style-type: none"> Inspected relevant documentation (e.g., SOPs) to test if roles and responsibilities for implementation of the security policy requirements were defined and documented. 	
IS - 4	An information security education and awareness program that includes policy training and periodic security updates for Azure personnel has been established.	<ul style="list-style-type: none"> Inquired of management to gain an understanding of the processes for awareness and training on information security for employees, contractors, and third-party users. Inspected training material to ascertain that it incorporated security policy requirements, and was updated as needed. Inspected the training material related to datacenter personnel and ascertained that it incorporated awareness on security risks and was updated as needed. 	No exceptions noted.

Operator Access

Control Objective 2: Controls provide reasonable assurance that logical access to production infrastructure is restricted to authorized personnel.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 1	Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities.	<ul style="list-style-type: none">• Inquired of management to understand the procedures in place for accessing the Azure production environment, including data backups and datacenters.• For a sample of Azure services, obtained and inspected authentication mechanisms and associated security groups to ascertain that privileged access to the Azure Management Portal and other administrative tools required authentication and was restricted to authorized entities based on job responsibilities.• Obtained and inspected a list of users with privileged access and ascertained that user access to the relevant domains was restricted to defined security user groups and membership.• Obtained and inspected the current listing of user accounts, including their respective user IDs within the Azure domains, and ascertained that each user was assigned a unique user ID which clearly identifies the user.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 2	Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.	<ul style="list-style-type: none"> Inquired of management if access requests require approval by the security group owner or asset owner using the account management tool. For a sample security group, observed the approval rules configuration and enforcement of approval rules for an access request. For a sample of security groups / individual user access, obtained and inspected approvals prior to provisioning access to specific applications or information resources. 	No exceptions noted.
OA - 3	Procedures to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place.	<ul style="list-style-type: none"> Inquired of the Operations team if procedures for disabling terminated user accounts within a defined time period after the user's termination date are established. Selected a sample of terminated users and inspected Active Directory (AD) domain logs showing that corporate accounts and AD production domain accounts were disabled within five days of the user's termination date. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 4	<p>User credentials adhere to established corporate standards and group policies for password requirements:</p> <ul style="list-style-type: none"> - expiration - length - complexity - history <p>Initial passwords have secure mechanisms in place for distribution and first-time use. For production domains where passwords are not in use, multi-factor authentication is enforced.</p>	<ul style="list-style-type: none"> • Inquired of management to gain an understanding of the implementation of password standards (e.g., length, complexity, age) and acceptable use guidelines for user credentials created on production domains where passwords are in use. • Obtained and inspected the group policies enforced on the corporate domain and production domains where passwords are in use. • For production domains where passwords are not in use, observed use of multi-factor authentication with a security PIN and certificate. • Inquired if temporary passwords were required to be changed on first use and expire on a timely basis. • Obtained sample notifications for the production domains and observed the security mechanisms in place for password distribution and first-time use. 	No exceptions noted.
OA - 5	<p>Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.</p>	<ul style="list-style-type: none"> • Inquired of management to gain an understanding of the process for performing periodic user access reviews for Microsoft Azure. • For a sample of managers reviewing Azure access, obtained and inspected the review log to ascertain whether reviews were performed for the managers' direct reports, and completed with implementation of identified changes. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 6	Production domain-level user accounts are disabled after 90 days of inactivity.	<ul style="list-style-type: none"> Inquired of the Cloud and Enterprise Security team if procedures for disabling user accounts that have been inactive for 90 days in the production environment are established. Obtained and inspected the configuration settings for applicable domains, to ascertain whether accounts are disabled after 90 days of inactivity. Obtained and inspected applicable domain user listings, including last login date and account status, to ascertain that there were no accounts that had been inactive for over 90 days. 	No exceptions noted.
OA - 7	Procedures for granting Azure personnel temporary access to customer data and applications, upon appropriate approval for customer support or incident handling purposes, have been established.	<ul style="list-style-type: none"> Inquired of management to understand the procedures in place for granting and revoking temporary access to internal administration services. For a sample of services, obtained and inspected temporary access logs and associated tickets to ascertain that temporary access was granted and approved per the defined process and had documented business justification associated with it. Observed the customer data access approval process and ascertained that Azure personnel can only obtain access to customer data after appropriate approval from the customers. 	No exceptions noted.

Operator Access

Control Objective 3: Controls provide reasonable assurance that logical access to production platform and network infrastructure is restricted to authorized personnel.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 1	Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities.	<ul style="list-style-type: none">• Inquired of management to understand the procedures in place for accessing the Azure production environment, including data backups and datacenters.• For a sample of Azure services, obtained and inspected authentication mechanisms and associated security groups to ascertain that privileged access to the Azure Management Portal and other administrative tools required authentication and was restricted to authorized entities based on job responsibilities.• Obtained and inspected a list of users with privileged access and ascertained that user access to the relevant domains was restricted to defined security user groups and membership.• Obtained and inspected the current listing of user accounts, including their respective user IDs within the Azure domains, and ascertained that each user was assigned a unique user ID which clearly identifies the user.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 2	Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.	<ul style="list-style-type: none"> Inquired of management if access requests require approval by the security group owner or asset owner using the account management tool. For a sample security group, observed the approval rules configuration and enforcement of approval rules for an access request. For a sample of security groups / individual user access, obtained and inspected approvals prior to provisioning access to specific applications or information resources. 	No exceptions noted.
OA - 3	Procedures to automatically disable Active Directory (AD) accounts and manually remove any non-AD accounts upon user's leave date are in place.	<ul style="list-style-type: none"> Inquired of the Operations team if procedures for disabling terminated user accounts within a defined time period after the user's termination date are established. Selected a sample of terminated users and obtained Active Directory (AD) domain logs showing that corporate accounts and AD production domain accounts were disabled within five days of the user's termination date. 	No exceptions noted.
OA - 5	Access privileges are reviewed quarterly to determine if access rights are commensurate to the user's job duties. Access is modified based on the results of the reviews.	<ul style="list-style-type: none"> Inquired of management to gain an understanding of the process for performing periodic user access reviews for Microsoft Azure. For a sample of managers reviewing Azure access, obtained and inspected the review log to ascertain whether reviews were performed for the managers' direct reports, and completed with implementation of identified changes. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 8	Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	<ul style="list-style-type: none"> Inquired of the process owners to understand the authentication enforced during an RDP session to production environment and encryption of an RDP session. Observed the authentication mechanisms and corresponding encrypted channel to ascertain that login attempt to remotely connect to the production environment was authenticated and over an encrypted connection. 	No exceptions noted.
OA - 9	User groups and Access Control Lists have been established to restrict access to network devices in the scope boundary.	<ul style="list-style-type: none"> Inquired of the Networking team if user groups and Access Control Lists (ACLs) are established to restrict access to network devices. Inquired if user groups were created and enforced via the Active Directory. Obtained and inspected configuration for a sample of network devices, and ascertained that TACACS+ / RADIUS was used for authentication and authorization of access, and that ACLs were applied. 	No exceptions noted.
OA - 10	Users are granted access to network devices in the scope boundary upon receiving appropriate approvals.	<ul style="list-style-type: none"> Inquired of the Networking team regarding the procedures in place to grant access to new users for network devices in the scope boundary. Observed the approval process to ascertain that access to a security group was granted upon approval from the network security group owner. For a sample of network security groups, sampled a user and ascertained that access was appropriate. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 13	Access to network devices in the scope boundary is restricted through a limited number of entry points that require authentication over an encrypted connection.	<ul style="list-style-type: none"> Inquired of the Networking team if access to the network devices is restricted through a limited number of entry points which require authentication over an encrypted Remote Desktop connection. Inspected the Network Account Management SOP and ascertained that procedures to restrict user access to network devices in the scope boundary, through a limited number of entry points that required authentication over an encrypted connection were established. For a sampled hop-box server, through observation, ascertained that remote access to network devices involved logging into a hop-box server using domain credentials and a smart card followed by a log in to the internal-facing terminal server using domain credentials. Also, noted that Secure Shell (SSH) was enforced to access the network device. Obtained and inspected IP addresses associated with a sample of hop-box servers and ascertained that the IP addresses allocated were restricted to a specific subnet for each instance of Azure cloud. Obtained and inspected configuration for a sample of network devices and ascertained that device access was restricted via above terminal servers. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 14	Access to network devices in the scope boundary requires two-factor authentication and / or other secure mechanisms.	<ul style="list-style-type: none"> Inquired of the Networking team if two-factor authentication is enforced for connecting to a network device. For a sampled network device, observed that logging in to the network device required two-factor authentication. Obtained and inspected configuration for a sample of network devices, and ascertained that authentication was enforced via TACACS+ or RADIUS servers. 	No exceptions noted.
OA - 15	Passwords used to access Azure network devices are restricted to authorized individuals based on job responsibilities and changed on a periodic basis.	<ul style="list-style-type: none"> Inquired of the Networking Team to gain an understanding of how passwords used to access network devices are restricted and rotated. Obtained and inspected tickets / rotation logs for sampled network devices to ascertain that the passwords for network devices were rotated as per the defined cadence. Observed that passwords were stored in secret repositories with access restricted to authorized individuals based on job responsibilities. 	Exception Noted: 33 out of 49 sampled network devices were not rotated as per the password rotation cadence defined in the documented procedures.
OA - 16	Network filtering to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components is implemented.	<ul style="list-style-type: none"> Inquired of management regarding the packet filtering mechanisms implemented to restrict incoming and outgoing traffic. Obtained and inspected the configuration files for sampled nodes and ascertained that filtering mechanisms and rules were configured to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 17	External traffic to the customer VM(s) is restricted to customer - enabled ports and protocols.	<ul style="list-style-type: none"> Inquired of management regarding network access controls in place to restrict external traffic to ports and protocols defined and enabled by customers. Attempted to access a sample set of VMs and observed that access was restricted based on the external traffic rules for ports and protocols enabled within the service configuration. 	No exceptions noted.
OA - 18	Azure network is segregated to separate customer traffic from management traffic.	<ul style="list-style-type: none"> Inquired of management regarding the procedures and technical controls used for segregating networks within the Azure environment. Obtained and inspected mechanisms used for segregating and restricting network traffic within the Azure environment. 	No exceptions noted.
OA - 19	Microsoft Azure has published virtualization industry standards supported within its environment.	<ul style="list-style-type: none"> Inquired of the Azure Operations team to understand the various published virtualization industry standards supported within the Azure environment, and solution-specific virtualization hooks available for customer review. Reperformed the control to ascertain that Azure published virtualization formats (e.g., Open Virtualization Format (OVF)) supported interoperability with third-party products such as Oracle Virtual Box, VMware Workstation, and XenSource. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 20	Alerts are generated when a break-glass account is used to access a production subscription.	<ul style="list-style-type: none"> Inquired of management to understand the procedures in place for monitoring break-glass account access to the production environment. Obtained and inspected the configuration files to ascertain that automated mechanisms were in place to generate alerts when a break-glass account is used to access the production environment. 	<p>Exception Noted:</p> <p>For two of four production domains that contain break-glass accounts, configuration related to generation of alerts was not in place and thus changes to the production environment made by these accounts would not have been monitored during the portion of the period July 1, 2022 to September 30, 2022.</p> <p>Additionally, tested the configurations related to generation of break-glass alerts on all the four production domains subsequent to September 30, 2022 and no additional exceptions were noted.</p>

Control ID	Control Activity	Test Procedures	Results of Tests
OA - 21	Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access.	<ul style="list-style-type: none"> Inquired of management to understand the process of using Secure Admin Workstation (SAW) machine and authentication using MFA for accessing production resources. Observed the access and authentication mechanisms to ascertain that access to production resources required using Secure Admin Workstation (SAW) machine and MFA for authentication. 	No exceptions noted.
DS - 16	Each Online Service's customer's data is segregated from other Online Services' customers' data, either logically or physically.	<ul style="list-style-type: none"> Performed inquiry of the service owner to understand how the AAD Distributed Directory Services environment enforces logical or physical segregation of customer data. Reperformed the control using test domains to ascertain that customer (tenant) data was segregated. 	No exceptions noted.

Data Security

Control Objective 4: Controls provide reasonable assurance that the data and secrets associated with the service are protected during transit and while at rest.

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 1	Cryptographic certificates, keys, and customer access keys used for communication between Azure services and other internal components are stored securely and are rotated on a periodic basis.	<ul style="list-style-type: none">Inquired of the Azure Operations team to understand the different types of cryptographic certificates and keys used by the services to connect to internal components, and their cadence / frequency of rotation.Observed the security of the cryptographic certificates and keys, and the process for periodic rotation. Additionally, ascertained through inspection of security group membership that the security groups granting access to the secrets were restricted to those personnel having valid business justification for access.For a sample of services, obtained and inspected evidence (e.g., tickets, logs) indicating if the secrets were rotated based on the pre-determined frequency.Performed inquiry and ascertained that the master key was secured based on controlled procedures.	<p>Exception Noted:</p> <p>Two of 26 sampled secrets were not rotated as per the secret rotation cadence defined in the documented procedures during the portion of the period July 1, 2022 to March 31, 2023.</p> <p>Additionally, tested 8 sampled secrets subsequent to March 31, 2023 and no additional exceptions were noted.</p>

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 2	<p>Customer data communicated through Azure service interfaces is encrypted during transmission over external networks.</p> <p>Location-aware technologies are implemented within the Azure portal to identify and validate authentication sessions.</p>	<ul style="list-style-type: none"> Inquired of the Azure Operations team to understand the controls in place that restrict transmission of customer data to secure protocols through various endpoints over external networks, and location-aware technologies which are implemented within the Azure Portal. Reperformed the control to ascertain that restrictions were in place to prevent use of insecure protocols (e.g., HTTP) for transmission of customer data over external networks, and location-aware technologies were implemented within the Azure Portal to identify and validate authentication sessions. 	No exceptions noted.
DS - 3	<p>Internal communication between key Azure components where customer data is transmitted / involved is secured using encryption.</p>	<ul style="list-style-type: none"> Inquired of the Azure Operations team to understand the use of secure mechanisms such as encryption for communication between internal Azure components that involves customer data. For a sample of Azure platform components, inspected configurations and observed the use of secure encryption mechanisms for internal communication. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 4	<p>Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures. The policies and procedures include the key rotation, archival and deactivation processes.</p> <p>Keys must have identifiable owners (binding keys to identities) and key management policies.</p>	<ul style="list-style-type: none"> Inquired of management regarding the policies and procedures in place for using cryptographic controls within the Azure environment. For a sample of major releases, ascertained that cryptographic policy requirements were enforced and required approvals were obtained for exceptions. For a sample of secrets from different Azure services, obtained and inspected secret configuration to ascertain that secrets were stored under service specific vaults or configuration files. 	No exceptions noted.
DS - 5	<p>Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.</p>	<ul style="list-style-type: none"> Inquired of management if backups of key Azure service components and secrets are performed regularly and stored in fault tolerant facilities. Obtained and inspected configurations and logs to ascertain that platform data and secrets data were replicated, backed up, and stored in separate locations. Obtained and inspected sample IcM tickets generated to ascertain that backup errors were investigated and remediated appropriately. 	No exceptions noted.
DS - 6	<p>Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.</p>	<ul style="list-style-type: none"> Inquired about the redundancy mechanisms in place for key components within the production environment. For a sample of platform components, inspected configurations and ascertained that redundancies were implemented within the production environment. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 7	Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.	<ul style="list-style-type: none"> Inquired about the redundancy mechanisms in place to replicate data stored across Azure services. For a sample of Storage accounts and SQL Databases, inspected configurations and ascertained that data was replicated across multiple nodes. Obtained and inspected configurations for the sampled services to determine geographical region of the data processing and storage. 	No exceptions noted.
DS - 8	Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.	<ul style="list-style-type: none"> Inquired of the DPS team regarding the process for scheduling of backups of production database based on customer requests. Inquired if backup of customer data was performed based on a defined schedule in accordance with documented operating procedures. Additionally, inspected the procedures to ascertain that retention of backup data was consistent with the security categorization assigned to it. For a sample of backup scheduling requests, obtained and inspected backup logs and ascertained that they were completed in accordance with customer requests and documented operating procedures. For a sample of backup failures, obtained tickets / backup status showing resolution details. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 9	Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.	<ul style="list-style-type: none"> Inquired of the DPS team if backup data integrity checks are conducted as part of standard restoration activities. Obtained and inspected DPS operating procedures and ascertained that processes for completing restoration from backups were defined. Additionally, ascertained that a ticketing system was used for tracking restoration requests. For a sample of restoration requests, obtained and inspected restoration tickets to ascertain that backup data integrity checks were completed in accordance with the request and documented operating procedures. 	No exceptions noted.
DS - 10	Guidelines for the disposal of storage media have been established.	<ul style="list-style-type: none"> Inquired of management to understand the process for disposal of storage media. Obtained the population of storage media disposals performed during the examination period, and judgmentally selected a sample of disposals. For a sample of media disposal requests, obtained and inspected evidence (destruction certificates) to ascertain that they followed the standard disposal process. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 11	Data corresponding to Azure is backed up to another region other than the primary data location and retained as per the retention policy.	<ul style="list-style-type: none"> Inquired of the DPS team if processes for backups and retention to primary and secondary locations are established. Obtained and inspected population of storage accounts and ascertained that the process for backups and retention was documented. For a sample of storage policies, obtained and inspected backup and retention policy configurations, to ascertain that data is backed up and retained as per the retention policy. 	No exceptions noted.
DS - 13	Production data on backup media is encrypted.	<ul style="list-style-type: none"> Inquired of the DPS team if production data is encrypted prior to storage on backup media. For a sample of Azure blob servers, obtained and inspected data encryption configurations to ascertain that production data was encrypted. Obtained and inspected the configuration settings for a sample of backup encryption system instances to ascertain whether they are enabled to encrypt production data for tape backups. 	No exceptions noted.
DS - 14	Azure services are configured to automatically restore customer services upon detection of hardware and system failures.	<ul style="list-style-type: none"> Inquired about the failover mechanisms in place to automatically restore role instances upon detection of a hardware and system failure. For a sample of node instances, observed the health status and service healing history to ascertain that automatic restoration was occurring. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
DS - 15	Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.	<ul style="list-style-type: none"> Inquired about the policy and procedures in place for the removal / retention of customer data upon termination of subscription. Obtained and inspected customer documentation to ascertain that data removal / retention processes were addressed. For a subscription, ascertained that access to customer data was handled in accordance with Microsoft Online Services Terms upon termination of the subscription. 	No exceptions noted.
DS - 17	Azure provides customers the ability to manage their own data encryption keys.	<ul style="list-style-type: none"> Inquired of management regarding the policies and procedures in place for customers to manage their own data encryption keys within the Azure environment. Obtained and inspected the policy and procedure documentation to ascertain that the processes are in place for the customers to manage their own encryption keys. Reperformed the procedures in an Azure tenant to ascertain that customers are able to manage their own encryption keys. 	No exceptions noted.
DS - 18	Microsoft performs a risk assessment for encryption and key management to evaluate changes and updates to cryptography controls.	<ul style="list-style-type: none"> Inquired of management on the policy and procedures in place for performing the risk assessments for changes and updates to encryption, key management and cryptography controls. Obtained and inspected meeting invites and meeting minutes of sampled crypto board meetings to ascertain that risk assessment is performed for changes identified for encryption, key management and cryptography controls. 	No exceptions noted.

Change Management

Control Objective 5: Control policies and procedures provide reasonable assurance that changes to the production platform are documented, authorized, and tested.

Control ID	Control Activity	Test Procedures	Results of Tests
CM - 1	Procedures for managing different types of changes to the Azure platform have been documented and communicated.	<ul style="list-style-type: none">Inquired of management regarding the procedures for managing various types of changes to the Microsoft Azure environment including tracking, approval, and testing requirements.Obtained documentation of Change Management procedures. Inspected documentation and ascertained that procedures for requesting, classifying, approving and implementing all types of changes, including major release, minor release, hotfix, and configuration changes, were defined.	No exceptions noted.
CM - 2	Key stakeholders approve changes prior to release into production based on documented change management procedures.	<ul style="list-style-type: none">Inquired of management about the procedures for managing various types of changes to the Microsoft Azure environment, including approval requirements.Identified and obtained the population of production deployments made during the examination period from the ticketing system, for the Microsoft Azure platform.Selected a sample of changes to production and ascertained that documented procedures for approval (including if the result of the risk assessment is documented appropriately and comprehensively and all changes were prioritized on the basis of the risk assessment) were followed prior to deployment.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
CM - 3	Responsibilities for requesting, approving, and implementing changes to the Azure platform are segregated among designated personnel.	<ul style="list-style-type: none"> Inquired of management if segregation of duties for key responsibilities for requesting, approving, and implementing changes to the Azure platform, is implemented. Identified and obtained the population of production deployments made during the examination period from the ticketing system, for the Microsoft Azure platform. Selected a sample of changes to production and ascertained that key responsibilities were segregated. 	No exceptions noted.
CM - 4	Software releases and configuration changes to the Azure platform are tested based on established criteria prior to production implementation.	<ul style="list-style-type: none"> Inquired of management about the procedures for managing various types of changes to the Microsoft Azure environment, including testing requirements. Identified and obtained the population of the production deployments made during the examination period from the ticketing system, for the Microsoft Azure platform. Selected a sample of changes to production and ascertained that documented procedures for testing were followed prior to deployment. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
CM - 5	Implemented changes to the Azure platform are reviewed for adherence to established procedures prior to closure. Changes are rolled back to their previous state in case of errors or security concerns.	<ul style="list-style-type: none"> Inquired of management regarding the procedures for reviewing implemented changes for adherence to established procedures prior to closure. Identified and obtained the population of production deployments made during the examination period from the ticketing system, for the Microsoft Azure platform. Selected a sample of changes to production and ascertained that roll back procedures were in place to roll back changes to their previous state in case of errors or security concerns. Selected a sample of changes to production and ascertained that changes were reviewed prior to closure. 	No exceptions noted.
CM - 6	Procedures to manage changes to network devices in the scope boundary have been established.	<ul style="list-style-type: none"> Inquired of the Networking team regarding the procedures established for managing changes to network devices in the scope boundary. Inspected network change management procedures, and for a sample of changes, obtained and inspected change management tickets to ascertain that documented procedures for managing changes to network devices including documentation, classification, review, testing and approval, were followed prior to deployment. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
CM - 7	Secure network configurations are applied and reviewed through defined change management procedures.	<ul style="list-style-type: none"> Inquired of the Networking team if the implementation and review of secure network configuration standards are followed through defined change management procedures. Inspected network configuration change management procedures and tested if change management procedures for secure network configuration changes were established. Obtained and inspected a sample of network change requests and ascertained that changes were documented, tested, reviewed, and approved based on the change type. 	No exceptions noted.
CM - 8	The Technical Security Services team develops security configuration standards for systems in the physical environment that are consistent with industry-accepted hardening standards. These configurations are documented in system baselines, are reviewed annually, and relevant configuration changes are communicated to impacted teams.	<ul style="list-style-type: none"> Inquired of the Cloud + AI Security team if security configuration standards for systems in the datacenters' environment are based on industry-accepted hardening standards and configurations are documented in system baselines and are reviewed annually. Relevant configuration changes are communicated to impacted teams. Inspected security configuration standards and technical baseline published in a central location and approvals related to an annual review and ascertained that technical baselines were consistent with the industry standard, approved, and the results were communicated to impacted teams. Selected a sample of servers and inspected their configuration to ascertain that documented security configuration standards and technical baseline were implemented. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
CM - 9	Datacenter change requests are classified, documented, and approved by the Operations Management Team.	<ul style="list-style-type: none"> Inquired of the Operations Management team if change requests are classified, documented, and approved by the Operations Management Team. Inspected procedures and tested if established procedures cover the process for requesting, documenting (including if the changes were assessed for risk and prioritized), classifying, approving, and executing datacenter changes. Selected a sample of change requests and tested that changes were classified, approved, and executed in accordance with documented procedures. 	No exceptions noted.
CM - 10	Secure configurations for datacenter software are applied through defined change management procedures including documentation, testing and approval.	<ul style="list-style-type: none"> Inquired of the Server Standards Team if server-based images are documented, tested and approved. Additionally, inquired if release to production is restricted to appropriate personnel. Obtained and inspected user access to the release production server and ascertained that access was restricted to appropriate personnel. Selected a sample of bugs and requirements from the releases during the period and inspected change tickets to ascertain that secure configurations for datacenter software were applied through defined change management procedures. 	No exceptions noted.
CM - 11	Change management processes include established workflows and procedures to address emergency change requests.	<ul style="list-style-type: none"> Inquired of management if procedures and workflows are established to address emergency change requests. Inspected the Change Management Procedures and tested that procedures and workflows were established to address emergency change requests. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
CM - 12	Azure has implemented tools to perform integrity verification checks to detect unauthorized changes to software, firmware and information.	<ul style="list-style-type: none"> Inquired of management regarding the tools implemented to detect unauthorized changes to software, firmware and information. For a sample of code integrity alerts, obtained and inspected logs and ascertained that the changes were identified by unique event IDs, and appropriate teams were notified to investigate and resolve identified items. 	No exceptions noted.
CM - 13	<p>Any changes to production via break-glass have been reviewed to ensure all changes were appropriate.</p> <p>Management monitors break-glass alerts on periodic basis to ensure that alerts are appropriately reviewed.</p>	<ul style="list-style-type: none"> Inquired of management to gain an understanding of the process related to performing review of changes made through break-glass accounts in the production environment. For all break-glass account access scenarios during the examination period, obtained and inspected tickets to ascertain that access was reviewed for appropriateness. For a sample of months, obtained and inspected evidence of monthly review of break-glass alerts by management to ascertain that break-glass alerts are appropriately reviewed by management. 	No exceptions noted.

Software Development

Control Objective 6: Controls provide reasonable assurance that development of new features or major changes to production platform follow a formal SDLC process and are documented, authorized and tested.

Control ID	Control Activity	Test Procedures	Results of Tests
SDL - 1	Development of new features and major changes to the Azure platform follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology.	<ul style="list-style-type: none">Inquired of management if the Microsoft SDL methodology for the development of new features and major changes to Microsoft Azure platform is followed.Obtained and inspected documentation to ascertain that an SDL methodology was defined to incorporate security practices as part of the development process.For a sample of changes made to production, obtained and inspected tickets to ascertain that documented procedures for testing were followed prior to deployment.	No exceptions noted.
SDL - 2	Applicable operational security and internal control requirements are documented and approved for major releases prior to production deployment.	<ul style="list-style-type: none">Inquired of management regarding the process to identify and document applicable operational security and internal control requirements as part of the SDL process.For a sample of major releases, ascertained that operational security and internal control requirements were identified, documented, and approved by designated owners.	No exceptions noted.
SDL - 3	Responsibilities for submitting and approving production deployments are segregated within the Azure teams.	<ul style="list-style-type: none">Inquired of the service teams if responsibilities for production deployment are segregated within the Microsoft Azure teams.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> For a sample of services, inspected access control lists to ascertain that segregation was maintained within the teams for submitting and approving production deployments and that the access to perform production deployments was restricted to authorized individuals within the Azure teams. 	
SDL - 4	New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments.	<ul style="list-style-type: none"> Inquired of the service teams if changes are developed and tested in separate environments prior to production deployment and production data is not replicated in test or development environments. For a sample of services, obtained and inspected subscription namespaces to ascertain that separate environments existed for development and testing of changes prior to production deployment. For the sampled services, inquired of service owners and inspected policies, test scripts, or configuration files, as applicable, to ascertain that production data is not replicated to the test or development environments. For a sample of changes made to production, obtained and inspected tickets to ascertain that documented procedures for testing were followed prior to deployment. 	No exceptions noted.
SDL - 5	A centralized repository for managing source code changes to the Azure platform is used. Procedures to authorize Azure personnel to submit source code changes based on their role, are established. Code changes submitted to the centralized repository are logged and can be	<ul style="list-style-type: none"> Inquired of the service teams about the access control procedures for source code repository. For a sample of services, obtained and inspected security groups and membership to ascertain that access to the source code repository was restricted to authorized Azure personnel. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	traced to the individuals or system components executing them.	<ul style="list-style-type: none"> For a sample source code repository, observed the configuration files and a change to ascertain that the identity of the individual and / or system component changing the code, the time of the change, and changes submitted to the source code repository are logged. 	
SDL - 6	Source code builds are scanned for malware prior to release to production.	<ul style="list-style-type: none"> Inquired of the service teams regarding the procedures in place to scan source code builds for malware. For a sample of source code builds, obtained and inspected evidence of scan build for malwares to ascertain that malware scanning was performed automatically as part of the build process prior to release to production. 	No exceptions noted.
SDL - 7	The SDL review for each service with a major release is performed and completed on a semi-annual basis, and signed off on by designated owners.	<ul style="list-style-type: none"> Inquired of management if an SDL review is performed at least semi-annually for each service with a major release and signed off by designated owners. For a sample of services, obtained and inspected relevant SDL tickets with review and sign-off details to ascertain that an SDL review was completed in the past six months as per the SDL methodology, and sign-offs were obtained from designated owners. 	No exceptions noted.

Vulnerability Management

Control Objective 7: Controls provide reasonable assurance that the production platform is monitored for known security vulnerabilities and potential unauthorized activity.

Control ID	Control Activity	Test Procedures	Results of Tests
VM - 1	Azure platform components are configured to log and collect security events.	<ul style="list-style-type: none">• Inquired of management regarding security event logging configured for Azure services to enable detection of potential unauthorized or malicious activities.• For a sample of services, obtained and inspected configurations and logs to ascertain that logging of key security events was enabled per documented procedures.• Inspected configurations and a sample notification to corroborate that security events generated alerts based on defined rulesets.• Observed the monitoring configuration to ascertain that a mechanism was in place to detect and resolve the activation or stopping of the logging process.	No exceptions noted.
VM - 2	Administrator activity in the Azure platform is logged.	<ul style="list-style-type: none">• Inquired of management regarding the mechanisms that are in place for logging administrator activities within Azure Service platform.• For a sample of services, obtained and inspected security logs to ascertain that administrator events were logged to the centralized monitoring infrastructure.	No exceptions noted.
VM - 3	A monitoring system to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries has been implemented.	<ul style="list-style-type: none">• Inquired of management regarding the monitoring capabilities within the Azure environment to detect potential malicious activities and intrusions.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> For a sample of services, inspected logs to ascertain that malicious activities were monitored as per the process. Additionally, inspected anti-malware event logging and the status of anti-malware engine signatures to corroborate that they were up to date. 	
VM - 4	Procedures to investigate and respond to malicious events detected by the Azure monitoring system in a timely manner have been established.	<ul style="list-style-type: none"> Inquired of the Microsoft Azure Incident Management Leads to ascertain that incidents and malicious events are identified, tracked, investigated, and resolved in a timely manner per documented procedures. Obtained and inspected a sample of incident tickets pertaining to the Azure Services and ascertained that incidents and malicious events were monitored, identified, tracked, investigated, and resolved. 	No exceptions noted.
VM - 5	Procedures to evaluate and implement Microsoft-released patches to Service components have been established.	<ul style="list-style-type: none"> Inquired of management regarding the patch management process within the Azure environment. Inspected patch management SOP and ascertained that procedures for evaluating and implementing relevant security patches within the Azure environment were established. For a sample of servers, obtained and inspected logs and patch details to ascertain that a selection of patches was assessed and implemented into the production environment per documented procedures. 	No exceptions noted.
VM - 6	Procedures to monitor the Azure platform components for known security vulnerabilities have been established. Identified	<ul style="list-style-type: none"> Inquired of management if processes to monitor and remediate known security vulnerabilities on the Azure platform are in place. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	security vulnerabilities are remediated.	<ul style="list-style-type: none"> Obtained and inspected the Vulnerability Risk Management SOP and ascertained that procedures for scanning and remediating vulnerabilities identified on servers have been established. For a sample of Azure platform components, obtained and inspected scan results to ascertain the components were monitored for security vulnerabilities. Further, ascertained that identified security vulnerabilities were remediated. 	
VM - 7	Procedures to configure and monitor network devices in the scope boundary, and resolve issues, have been established.	<ul style="list-style-type: none"> Inquired of the Networking team to ascertain that procedures for configuring and monitoring network devices in the scope boundary are established, and that identified issues are resolved. Obtained and inspected documentation and ascertained that procedures related to network infrastructure were established and included network device access, configuration management, network device change management, Access Control List (ACL) change management, and ACL triage process. Additionally, ascertained that the procedures were reviewed by the Networking team management on an annual basis. For a sample of network devices in the scope boundary, obtained and inspected device configurations to ascertain that the devices were in compliance with established standards. For devices that were not in compliance, ascertained that issues were investigated and resolved. 	No exceptions noted.
VM - 9	Network devices in the scope boundary are configured to log and collect security events, and	<ul style="list-style-type: none"> Inquired of the Networking team to ascertain that network devices in the scope boundary are configured to log and collect security events, and monitored for compliance. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	monitored for compliance with established security standards.	<ul style="list-style-type: none"> For a sample of network devices in the scope boundary, obtained and inspected device configurations to ascertain that they were configured to log and collect security events, with event logs routed to designated log servers. Inspected configuration compliance reports for the sampled network devices, and ascertained that scans were configured per established security standards. For devices identified by scanning as not being in compliance, ascertained that issues were investigated and resolved. 	
VM - 10	Azure provides logging mechanisms that can be configured by customers to log activities and performance metrics.	<ul style="list-style-type: none"> Inquired of management to understand the logging mechanisms available to customers, and how these logging mechanisms can be leveraged. Reperformed the control to ascertain that logging mechanisms can be configured by customers to log activities and performance metrics. Inspected the logs available on the portal and ascertained that expected entries are being logged. 	No exceptions noted.
VM - 11	Microsoft operating system updates for virtual machines are made available through Microsoft Security Response Center (MSRC) site and Windows Update.	<ul style="list-style-type: none"> Inquired of management regarding the mechanisms to update the Microsoft operating system installed on virtual machines through the Microsoft Security Response Center (MSRC) and Windows Update. Inspected the MSRC to ascertain that updates to the Microsoft operating system on virtual machines are available through the MSRC. Accessed Windows Update and observed that customers can configure virtual machines to update operating systems as needed. Reperformed by configuring automatic updates and through inspection ascertained that updates were applied as a result. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
VM - 12	The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard.	<ul style="list-style-type: none"> Inquired of management to understand the processes followed and tools used by the services for monitoring service availability and communicating service availability status to customers through Service Dashboard. For a sample of services, inspected monitoring tools and configurations to ascertain that the availability tools were implemented to monitor service availability and generate real-time alerts to notify the designated personnel of any issues. Inspected the Service Dashboard to ascertain the availability status of services were accurately reflected. 	No exceptions noted.
VM - 13	Vulnerabilities for network devices are evaluated and mitigated based on documented procedures.	<ul style="list-style-type: none"> Inquired of management if documented procedures are followed when remediating vulnerabilities on network devices. Obtained and inspected documentation to ascertain if procedures to evaluate vulnerability risks have been established. For sampled network devices, selected a sample of vulnerabilities and their corresponding remediation procedures to ascertain if applicable and defined mitigation procedures were implemented. 	No exceptions noted.

Incident Management

Control Objective 8: Controls provide reasonable assurance that production incidents are identified and responded to in accordance with documented procedures for timely resolution.

Control ID	Control Activity	Test Procedures	Results of Tests
IM - 1	An incident management framework with defined processes, roles, and responsibilities for the detection, escalation and response of incidents, has been established and communicated.	<ul style="list-style-type: none">• Inquired if information security incidents are managed through designated responsibilities and documented procedures.• Obtained and inspected information security incident management procedures and ascertained that roles and responsibilities for escalation and notification to specialist groups during a security incident were established and communicated.	No exceptions noted.
IM - 2	Events, thresholds, and metrics have been defined and configured to detect incidents and alert the associated Operations team.	<ul style="list-style-type: none">• Inquired if events, thresholds and metrics are established to detect and facilitate an alert / notification to incident management teams.• Observed the configuration files and ascertained that automated monitoring and notification was configured for predefined events.• For a sample of platform components, ascertained that automated notifications were received upon the occurrence of an event meeting the configured specifications.	No exceptions noted.
IM - 3	The Operations team performs monitoring, including documentation, classification, escalation, and coordination of incidents per documented procedures.	<ul style="list-style-type: none">• Inquired about the procedures for 24x7 monitoring and handling of incidents.• Identified the population of incidents (all severities) in the examination period and obtained and inspected the incident tickets for a sample to ascertain that each incident was handled per documented procedures.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> Inspected a sample of incident tickets and ascertained that there is monitoring of alerts and notification of potential incidents. Obtained and inspected Monitoring team schedules to ascertain that there was 24x7 monitoring. 	
IM - 4	Incident post-mortem activities for severe incidents impacting the Azure environment are conducted.	<ul style="list-style-type: none"> Inquired if a post-mortem is performed for customer impacting severity 0 and 1 incidents and a formal report is submitted for management review and that mechanisms are in place to track and remediate recurring incidents. Inspected a sample of incidents to ascertain that post-mortem was performed as per documented procedures. 	No exceptions noted.
IM - 5	The Cyber Defense Operations Center (CDOC) team provides reports of information security events to Cloud + AI management on a quarterly basis. Problem statements for systemic issues are submitted to executive leadership for review.	<ul style="list-style-type: none"> Inquired of the Cyber Defense Operations Center (CDOC) team if information security review report is presented to Cloud + AI management on a quarterly basis. Obtained and inspected a sample of quarterly reports and ascertained that problem statements for systemic issues were submitted for executive leadership review. Obtained and inspected evidence (such as meeting invite, list of attendees) to ascertain that the report was reviewed by executive leadership. 	No exceptions noted.
IM - 6	The Cyber Defense Operations Center (CDOC) team performs annual tests on the security incident response procedures.	<ul style="list-style-type: none"> Inquired of the Cyber Defense Operations Center (CDOC) team if incident response procedures are tested at least annually and the test results are documented in centralized tracking system. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> Obtained and inspected the documentation from the exercise conducted by the CDOC team including the test plan and testing results and noted that the tested action items, expected results, and actual results were included and documented. 	

Physical and Environmental Security

Control Objective 9: Control policies and procedures provide reasonable assurance that systems and data are protected against unauthorized physical access and environmental threats.

Control ID	Control Activity	Test Procedures	Results of Tests
PE - 1	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.	<ul style="list-style-type: none">Inquired of the Datacenter Management team if access levels are established and if physical access to the datacenter is restricted to authorized personnel.Inspected the datacenter SOPs and ascertained that procedures were in place to restrict physical access to the datacenter for employees, vendors, contractors, and visitors. Inquired of management regarding the review and communication of the procedures.Obtained and inspected a sample of access requests and ascertained that access requests were tracked using a centralized ticketing system and were authorized by the designated approvers.	No exceptions noted.
PE - 2	Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.	<ul style="list-style-type: none">Inquired of the Datacenter Management team if security verification and check-in procedures are established for personnel requiring temporary access to the interior datacenters.Inspected the datacenter SOPs and ascertained if procedures were in place for security verification, check-in, and escorting personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors.	No exceptions noted.
PE - 3	Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.	<ul style="list-style-type: none">Inquired of the Datacenter Management team if physical access to datacenters is reviewed and verified quarterly.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> Inspected Datacenter Services (DCS) operating procedures and ascertained that quarterly access review procedures were documented. For sampled quarterly access reviews, ascertained that reviews were completed appropriately. 	
PE - 4	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.	<ul style="list-style-type: none"> Inquired of the Datacenter Management team if physical access mechanisms to restrict access to authorized individuals are in place. For a sample of datacenters, observed that access to the main entrance of the datacenter, exterior doors, co-locations, and other interior rooms within the datacenter was restricted through physical access mechanisms (such as electronic card readers, biometric handprint readers, or man traps). Observed attempts to access restricted areas within the datacenters without appropriate level of access and ascertained that access was denied. 	No exceptions noted.
PE - 5	The datacenter facility is monitored 24x7 by security personnel.	<ul style="list-style-type: none"> Inquired of the Datacenter Management team if security personnel monitor the datacenter premises through a video surveillance system 24 hours a day, 7 days a week. Observed security personnel as well as video surveillance systems at a sample of datacenters and ascertained that views for facility entrances, exits, parking lots, doors, co-locations, restricted areas and / or loading / delivery docks were being monitored by security personnel using on-site security consoles. Requested surveillance tapes for a sample of datacenters and inspected that the tapes were 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		retained according to the documented operating procedures.	
PE - 6	Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.	<ul style="list-style-type: none"> Inquired of the Datacenter Management team if environmental equipment within datacenter facilities is maintained and tested according to documented policy and maintenance procedures. Inspected DCS operating procedures and ascertained that procedures were documented for maintaining adequate facility and environmental protection at the datacenters. For a sample of datacenters observed that the critical environment was being monitored. Inspected maintenance and testing records for a sample of on-site environmental equipment. 	No exceptions noted.
PE - 7	Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.	<ul style="list-style-type: none"> Inquired of the Datacenter Management team if environmental controls are implemented to protect systems inside the datacenters. For a sample of datacenters, observed that environmental controls including temperature control, HVAC (heating, ventilation and air conditioning), fire detection and suppression systems, and power management systems were in place. 	No exceptions noted.
PE - 8	Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident	<ul style="list-style-type: none"> Inquired of the physical security management team if an incident response procedure is established to address physical security incidents and methods to report security incidents, and these are reviewed and approved annually. Inspected the Incident Response Procedure and ascertained that the procedure was approved by appropriate Physical Security Managers and included 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	and the methods to report security weaknesses.	documentation of severity of events, procedures to be followed in the event of a physical security incident and guidelines for emergency communication and reporting.	

Logical Access

Control Objective 10: Controls provide reasonable assurance that logical access to customer data and systems within the Service is restricted.

Control ID	Control Activity	Test Procedures	Results of Tests
LA - 1	External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings.	<ul style="list-style-type: none">• Inquired of the service teams to understand the mechanisms implemented to allow customers to configure access or traffic restrictions.• Reperformed the control for a sample of services to ascertain that access to the service was restricted based on the customer configured authentication and authorization settings.	No exceptions noted.
LA - 2	Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time.	<ul style="list-style-type: none">• Inquired of the service teams regarding controls in place to ascertain the following requirements:<ul style="list-style-type: none">– New passwords within Azure conform to the applicable password policy requirements– Users are forced to change the password when using them for the first time– Temporary credentials assigned to users by the service expire within 14 days• Reperformed the control for a sample of services through various scenarios such as:<ul style="list-style-type: none">– Providing sample weak passwords– Tampering with the Hypertext Transfer Protocol (HTTP) request by using weak passwords– Using expired passwords to ascertain that new password(s) that did not meet applicable password policy requirements were not accepted.	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
LA - 3	Logical segregation to restrict unauthorized access to other customer tenants is implemented.	<ul style="list-style-type: none"> Inquired of the service teams to understand the segregation controls implemented to restrict unauthorized access to other customer tenants. Reperformed the control for a sample of services to ascertain that segregation was enforced between the tenants, and that customers could access the data within the service only after the required authorization checks. 	No exceptions noted.
LA - 4	Customer data that is designated as "confidential" is protected while in storage within Azure services.	<ul style="list-style-type: none"> Inquired of the service teams to understand the controls implemented to protect customer confidential data stored within the service. Reperformed the control for a sample of services to ascertain that customer confidential data stored within the service was protected. 	No exceptions noted.
LA - 5	User sessions within Azure can be configured by customers to expire after a stipulated period of inactivity.	<ul style="list-style-type: none"> Inquired of management to understand the mechanisms implemented to enforce session timeout. Reperformed the control to validate that: <ul style="list-style-type: none"> Sessions are invalidated after an idle timeout as configured by the user or tenant administrator. Session remains active if timeout is set to 'never' after a long duration. 	No exceptions noted.
LA - 6	The jobs configured by the customer administrators are executed within thirty (30) minutes of the scheduled job run and are repeated based on the defined recurrence settings.	<ul style="list-style-type: none"> Inquired of the service teams to understand the mechanisms in place to execute jobs, configured by the customer administrators, within thirty (30) minutes of the scheduled job run and repeat based on the defined recurrence settings. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> Reperformed the control for a sample job to ascertain that jobs configured by the customer administrators were executed within thirty (30) minutes of the scheduled job run and were repeated based on the defined recurrence settings. 	
LA - 7	Quotas on Azure services are enforced as configured by the service administrators to protect against availability related issues.	<ul style="list-style-type: none"> Inquired of the service teams to understand the mechanisms in place that allow customers to implement quotas on the service. Reperformed the control for a sample of services by accessing the Azure Management Portal using a subscription, and ascertained that quotas and rate limits were enforced as configured. 	<p>Exception Noted:</p> <p>For two of 19 sampled offerings, quota restrictions were not configured as per the defined limits during the portion of the period July 1, 2022 to March 31, 2023.</p> <p>Additionally, tested four sampled offerings subsequent to March 31, 2023 and no additional exceptions were noted.</p>
LA - 8	The private root key belonging to the Azure services is protected from unauthorized access.	<ul style="list-style-type: none"> Inquired of the service teams regarding the controls in place to protect the private root key, belonging to Azure services, from unauthorized access. Obtained and inspected security plan for the physical location where private root keys are stored to ascertain that security procedures were established to protect the root key from unauthorized logical or physical access. For a sample of access requests to the root key, obtained access notification and approval to 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		ascertain that access to root keys were authorized and approved.	
LA - 9	<p>Service initializes the resource groups within the management portal based on the customer configured templates.</p> <p>Service allows customers to monitor and control the distribution of system resources created within the resource group in order to prevent resources from being congested.</p>	<ul style="list-style-type: none"> Inquired of the service team to understand the mechanisms in place to initialize resource groups within the Azure Management Portal based on the customer configured templates and the mechanisms in place to monitor and control the distribution of the system resource created within the resource group. Reperformed the control using a subscription and ascertained that the service was initialized based on customer configured templates. Reperformed the control to ascertain that the distribution of the system resource created within a resource group can be monitored and controlled by customers. 	No exceptions noted.
LA - 10	The errors generated during the job execution are monitored and appropriate action is taken based on the job settings defined by the customer administrator.	<ul style="list-style-type: none"> Inquired of the service teams regarding monitoring of errors generated during the job execution and actions taken based on the job settings defined by the customer administrator. Reperformed the control for a sample of services to ascertain that errors generated during the job execution were monitored and actions were taken based on the job settings defined by the customer administrator. 	No exceptions noted.
LA - 11	One Time Passwords (OTPs) used for self-service password reset are randomly generated. OTPs expire after a pre-defined time limit. OTPs sent to the customer administrator are required to be validated before a	<ul style="list-style-type: none"> Inquired of the service team regarding the controls in place that: <ul style="list-style-type: none"> Facilitate random generation of OTPs Expire OTPs after their usage or after a pre-defined time limit Validate the OTPs before the password is reset 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
	password change is allowed. SSPR does not display user identifiable information during the password reset. Azure Active Directory password policy requirements are enforced on the new passwords supplied by customer administrators within SSPR portal. New passwords supplied by customer administrators are protected during transmission over external networks.	<ul style="list-style-type: none"> - Restrict transmission of new passwords to secure protocols through various endpoints over external networks - Validate if new passwords within the SSPR portal conform to the Azure Active Directory (Azure AD) password policy requirements • Reperformed the control and obtained sample SMS and email OTPs to ascertain that the characters in the SMS and email were random. • Reperformed the control for various scenarios such as: <ul style="list-style-type: none"> - Reusing OTP after initially using it to reset passwords - Using OTP after expiration of the pre-defined time limit <p>to ascertain that OTPs expired after a pre-defined time limit, and OTPs sent to the customer administrator were required to be validated before password was allowed to be changed.</p> <ul style="list-style-type: none"> • Reperformed the control to ascertain that restrictions were in place to prevent use of insecure protocols (e.g., HTTP) for transmission of new passwords over external networks. • Reperformed the control through various scenarios such as: <ul style="list-style-type: none"> - Providing sample weak passwords through portal <p>to ascertain that new passwords that did not meet necessary password policy requirements were not accepted by the SSPR portal.</p>	

Control ID	Control Activity	Test Procedures	Results of Tests
LA - 12	Images may be customized and access to images may be restricted by the customer. Updates to available images are communicated to through customer-facing websites.	<ul style="list-style-type: none"> Inquired of the service team to understand how image access can be restricted, customized, and how updates are communicated to customers. Reperformed the control by creating a customized image and restricting access to the image through the Azure portal. Inspected communications of updates on customer-facing websites and also inspected the Azure Marketplace and ascertained that a selection of hardened images was available. 	No exceptions noted.
ED - 1	Production servers that reside in edge locations are encrypted at the drive level.	<ul style="list-style-type: none"> Inquired of the Front Door team to gain an understanding of the encryption mechanism present at the drive level on production servers. For a sample of production servers, ascertained that BitLocker was running and the Trusted Platform Module (TPM) was enabled. 	No exceptions noted.
ED - 2	Intrusion alerts are sent to the operator when physical access to the production servers that reside in edge locations is detected.	<ul style="list-style-type: none"> Inquired of the Front Door team to understand the mechanism for detecting and alerting unauthorized physical access to production servers. For a sample of production servers, obtained and inspected hardware specifications to ascertain that intrusion detection switches were present for the devices and inspected configurations to ascertain that they were enabled and configured to generate alerts upon detecting an intrusion. 	No exceptions noted.
ED - 3	All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level.	<ul style="list-style-type: none"> Inquired of the Front Door team to understand the configuration settings used to disable unused IO ports on production servers. 	No exceptions noted.

Control ID	Control Activity	Test Procedures	Results of Tests
		<ul style="list-style-type: none"> Obtained and inspected the configuration files for a sample of servers and ascertained that selected IO ports were disabled on the servers. 	

Section V:
Supplemental Information
Provided by Microsoft

Section V: Supplemental Information Provided by Microsoft

The following information is provided for informational purposes only and has not been subjected to the procedures applied in the examination. Accordingly, Deloitte & Touche LLP expresses no opinion on the following information.

Azure Compliance

Microsoft Azure supports compliance with a broad set of industry-specific laws and meets broad international standards. Azure has ISO 27001, ISO 27017, ISO 27018, ISO 22301, and ISO 9001 certifications, PCI DSS Level 1 validation, SOC 1 Type 2 and SOC 2 Type 2 attestations, HIPAA Business Associate Agreement, and HITRUST certification. Operated and maintained globally, Microsoft Azure is regularly and independently verified for compliance with industry and international standards, and provides customers the foundation to achieve compliance for their applications. More information is available from the [Azure Compliance](#) site.

Infrastructure Redundancy and Data Durability

Azure mitigates the risk of outages due to failures of individual devices, such as hard drives or even entire servers through the following:

- Data durability of Azure Storage (Blobs (including Azure Data Lake Storage Gen2), Disks, Files, Queues, Tables) including Cool and Premium, facilitated by maintaining redundant copies of data on different drives located across fully independent physical storage subsystems. Copies of data are continually scanned to detect and repair bit rot.
- Cloud Services availability, maintained by deploying roles on isolated groupings of hardware and network devices known as fault domains. The health of each compute instance is continually monitored and roles are automatically relocated to new fault domains in the event of a failure.
- Network load balancing, automatic OS and service patching is built into Azure. The Azure application deployment model also upgrades customer applications without downtime by using upgrade domains, a concept similar to fault domains, which helps ascertain that only a portion of the service is updated at a time.

Data Backup and Recovery

In addition to the core data durability built into Azure, Azure provides customers with a feature to capture and store point-in-time backups of their stored Azure data. This allows customers to protect their applications from an event of corruption or unwanted modification or deletion of its data.

Microsoft Azure E.U. Data Protection Directive

Microsoft offers contractual commitments for the safeguarding of customer data as part of the Online Services Terms (OST) [Microsoft Licensing Terms and Documentation](#).

- A Data Processing Agreement that details our compliance with the E.U. Data Protection Directive and related security requirements for Azure core features within ISO / IEC 27001:2013 scope.
- E.U. Model Contractual Clauses that provide additional contractual guarantees around transfers of personal data for Azure core features within ISO / IEC 27001:2013 scope.

Additional Resources

The following resources are available to provide more general information about Azure and related Microsoft services:

- Microsoft Azure Home - General information and links to further resources about Azure: <http://azure.microsoft.com>
- Microsoft Trust Center includes details regarding Compliance, Service Agreement and Use Rights, Privacy Statement, Security Overview, Service Level Agreements, and Legal Information <http://www.microsoft.com/en-us/trustcenter>
- Azure Documentation Center - Main repository for developer guidance and information: <https://azure.microsoft.com/en-us/documentation>
- Microsoft's Security Development Lifecycle - SDL is Microsoft's security assurance process that is employed during the development of Azure: <https://www.microsoft.com/en-us/securityengineering/sdl/>
- Microsoft's Global Datacenters is the group accountable for delivering a trustworthy, available online operations environment that underlies Microsoft Azure: <https://azure.microsoft.com/en-us/global-infrastructure/>
- Microsoft Security Response Center - Microsoft security vulnerabilities, including issues with Azure, can be reported to: <https://www.microsoft.com/en-us/msrc> or via email to secure@microsoft.com

Management's Response to Exceptions Noted

The table below contains Management's response to the exceptions identified in Section IV - Information Provided by Independent Service Auditor Except for Control Objectives and Control Activities above.

Control ID	Control Activity	Exception Noted	Management Response
OA - 15	Passwords used to access Azure network devices are restricted to authorized individuals based on job responsibilities and changed on a periodic basis.	33 out of 49 sampled network devices were not rotated as per the password rotation cadence defined in the documented procedures.	Management continues to be committed to implementing a process to rotate passwords, monitor, detect, and remediate bugs that cause the automated workflow to fail, resulting in some passwords not being rotated timely. Although evidence of password rotation could not be provided, the affected accounts can only be accessed when the central authentication system is down. As such, management deems there was no risk as a result of the exception.

Control ID	Control Activity	Exception Noted	Management Response
OA - 20	Alerts are generated when a break-glass account is used to access a production subscription.	<p>For two of four production domains that contain break-glass accounts, configuration related to generation of alerts was not in place and thus changes to the production environment made by these accounts would not have been monitored during the portion of the period July 1, 2022 to September 30, 2022.</p> <p>Additionally, tested the configurations related to generation of break-glass alerts on all the four production domains subsequent to September 30, 2022 and no additional exceptions were noted.</p>	<p>Management obtained access logs and reviewed the break-glass activity covering the impacted period. Per inspection of the logs, it was verified break-glass usage was limited for one domain. This domain is used to host a small quantity of services relative to the other domains where alerting was enabled. For the other domain, there were no instances of break-glass access. In addition, monitoring has since been enabled for these domains.</p> <p>For each instance of break-glass access, management obtained work items to corroborate the activity was pre-planned and authorized. During the analysis of the logs there were no instances of access where code deployments occurred. Although alerting was not enabled, management has multiple controls in place to address the risk of unauthorized changes to production through break-glass access included in the SOC report. Alerting on these two domains is now enabled.</p>
DS - 1	Cryptographic certificates, keys, and customer access keys used for communication between Azure services and other internal components are stored securely and are rotated on a periodic basis.	<p>Two of 26 sampled secrets were not rotated as per the secret rotation cadence defined in the documented procedures during the portion of the period July 1, 2022 to March 31, 2023.</p> <p>Additionally, tested 8 sampled secrets subsequent to March 31, 2023 and no additional exceptions were noted.</p>	Management has since either deleted the secret or rotated the password of the secret, validated that access is restricted to authorized personnel, and stored in an encrypted format. Additionally, the engineering team has performed a review over all their secrets and rotated them as needed.

Control ID	Control Activity	Exception Noted	Management Response
LA - 7	Quotas on Azure services are enforced as configured by the service administrators to protect against availability related issues.	<p>For two of 19 sampled offerings, quota restrictions were not configured as per the defined limits during the portion of the period July 1, 2022 to March 31, 2023.</p> <p>Additionally, tested four sampled offerings subsequent to March 31, 2023 and no additional exceptions were noted.</p>	Quota restrictions were not functioning as expected due to a bug which has since been resolved. There were no service outages or capacity issues with the offerings caused by the bug. Additionally, the offerings have monitoring mechanisms in place to detect if resources were not able to be created due to capacity constraints. As such, management deems there was no risk as a result of the exception.

User Entity Responsibilities

The following list includes user entity responsibilities that Microsoft assumes its user entities have implemented, but are not required to meet the control objectives:

- Customers are responsible for managing compliance with applicable laws / regulations.
- Customers are responsible for implementing workstation timeout for extended periods of inactivity.
- Customers are responsible for following appropriate security practices during development and deployment of their applications on Azure Web Apps.
- Customers are responsible for configuring their Web Apps deployments to log appropriate diagnostic information and monitoring for security related events.
- Customers are responsible for verifying the security of patching, and maintaining any third party applications and / or components that they install on the Azure production environment.
- Customer entities are responsible for notifying the MFA service of changes made to technical or administrative contact information.
- Customers are responsible for maintaining their own system(s) of record.
- Customers are responsible for ensuring the supervision, management and control of the use of MFA services by their personnel.
- Customers are responsible for developing their own Disaster Recovery and Business Continuity Plans that address the inability to access or utilize MFA services.
- Customers are responsible for ensuring that the data submitted to the MFA service is complete, accurate and timely.
- Customers are responsible for determining, implementing and managing encryption requirements for their data within the Azure platform where Azure does not enable it by default and / or can be controlled by the customer.
- Customers are responsible for determining the configurations to be enabled on their VMs.
- Customers are responsible for backup of their data from Azure to local storage upon Azure subscription termination.

- Customers are responsible for designing and implementing interconnectivity between their Azure and on-premises resources.
- Customers are responsible for specifying authorization requirements for their Internet-facing messaging end points.
- Customers are responsible for encrypting content using the SDK provided by Media Services.
- Customers are responsible for the rotation of DRM and content keys.
- Customers are responsible for following a Secure Development Lifecycle methodology for their applications developed on Azure.
- Customers are responsible for application quality assurance prior to promoting to the Azure production environment.
- Customers are responsible for monitoring the security of their applications developed on Azure.
- Customers are responsible for reviewing public Azure security and patch updates.
- Customers not signed up for auto-upgrade are responsible for applying patches.
- Customers are responsible for designing and implementing redundant systems for hot-failover capability.
- Customers are responsible to secure their API using mutual certificates, VPN or the Azure ExpressRoute service.
- Customers are responsible for using encrypted variable asset to store secrets while utilizing the Automation service.
- Customers are responsible for reviewing the access activities associated with their accounts and their VM applications.
- Customers are responsible for reviewing the access activities associated with their Intune enrolled devices.
- Customers are responsible for determining and implementing encryption requirements for their Intune enrolled devices and on-premises resources.
- Customers are responsible for determining the applications and policies to be deployed to their Intune enrolled devices.
- Customers are responsible for designing and implementing interconnectivity between their Intune subscription and on-premises resources (specifically any VPN infrastructure, System Center Configuration Manager infrastructure, and the Exchange Connector).
- Customers utilizing the Azure ExpressRoute service are responsible for ensuring their on-premises infrastructure is physically connected to their connectivity service provider infrastructure.
- Customers are responsible for ensuring the service with their connectivity provider is compatible with the Azure ExpressRoute service.
- Customers are responsible for ensuring that their connectivity provider extends connectivity in a highly available manner so that there are no single points of failure.
- Customers utilizing the Azure ExpressRoute service are responsible to set up redundant routing between Microsoft and the customer's network to enable peering.
- Customers co-located with an exchange or connecting to Microsoft through a point-to-point Ethernet provider are responsible to configure redundant Border Gateway Protocol (BGP) sessions per peering to meet availability SLA requirements for Azure ExpressRoute.
- Customers are responsible for appropriate setup and management of Network Address Translation (NAT) to connect to Azure services using Azure ExpressRoute.
- Customers are responsible for ensuring the NAT IP pool advertised to Microsoft is not advertised to the Internet when utilizing the Azure ExpressRoute service.

- Customers are responsible for adhering to peering requirements with other Microsoft Online Services such as Office 365 when utilizing the Azure ExpressRoute service.
- Customers utilizing the Azure ExpressRoute service are responsible for encrypting their data while in transit.
- Customers utilizing the Azure ExpressRoute service are responsible for protection of their Cloud Services and resource groups through use of appropriate security and firewalling.
- Customers are responsible for backing up keys that they add to Azure Key Vault.
- Customers are responsible for physically securing the StorSimple device in their premise.
- Customers are responsible for specifying strong cloud encryption key used for encrypting the data from their StorSimple device to the cloud.
- Customers are responsible for providing Internet connectivity for their StorSimple device to communicate with Azure.
- Customers are responsible to support timely incident responses with the Azure team.
- Customers are responsible for responding to data subject requests for customer data or system generated logs.